

PCT/JP 00/02041

30.03.00

JP00/02041
日本国特許

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 14 APR 2000

WIPO

PCT

EKU

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年 3月30日

出願番号

Application Number:

平成11年特許願第088346号

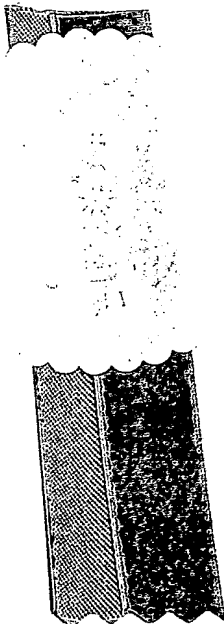
出願人

Applicant (s):

ソニー株式会社

**PRIORITY
DOCUMENT**

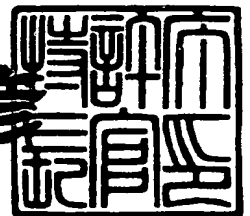
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)



2000年 1月28日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特2000-3001040

【書類名】 特許願

【整理番号】 9900210504

【提出日】 平成11年 3月30日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 石黒 隆二

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 河上 達

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 田辺 充

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 江面 裕一

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 河原 博和

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、情報処理システム、並びに提供媒体

【特許請求の範囲】

【請求項 1】 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置において、

前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信手段と、

前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と

前記記録手段に記録されている前記プログラムを、前記半導体 I C に送信する送信手段と

を含むことを特徴とする情報処理装置。

【請求項 2】 前記プログラムは、インタプリタに実行させるソースプログラムである

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記プログラムは、オブジェクトプログラムである

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置の情報処理方法において、

前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、

前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項 5】 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置に、

前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、前

記認証局から暗号化された前記プログラムを受信する通信ステップと、

前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体 I C に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項 6】 半導体 I C が装着され、前記半導体 I C に実行させるプログラムを供給する情報処理装置、および認証局からなる情報処理システムにおいて

前記情報処理装置は、

前記半導体 I C に実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信手段と、

前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体 I C に送信する送信手段と

を含み、

前記認証局は、

前記半導体 I C に実行させる前記プログラムを受信するとともに、前記情報処理装置に暗号化された前記プログラムを送信する通信手段と、

前記通信手段が受信した前記プログラムを所定の方式で暗号化する暗号化手段と

含むことを特徴とする情報処理システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、情報処理装置および方法、情報処理システム、並びに提供媒体に関し、特に、所定のデータを記憶し、所定の処理を行う情報処理装置および方法、

情報処理システム、並びに提供媒体に関する。

【0002】

【従来の技術】

最近、CD (Compact Disk)、MD (Mini Disk) といった音楽データをデジタル的に記録または再生することができる装置が普及してきた。その結果、このようなデジタル的に音楽データを記録再生できる装置をパーソナルコンピュータなどと組み合わせることで、デジタル音楽データを不正に複製することも比較的容易に行うことができるようになってきた。そこで、著作物としての音楽データを不正に複製することができないようにするために、各種の方法が提案されている。

【0003】

例えば、コピー元を制御するソフトウェアに、コピー先の装置と相互認証させ、適正な認証結果が得られたとき、音楽データを暗号化して、コピー先の装置に転送させ、コピー先の装置において、その暗号化されたデータを復号して利用するようにすることが提案されている。

【0004】

また、コピー元のソフトウェアに所定のハードウェアに記憶されているIDを利用して、コピー先の装置と相互認証させることも提案されている。

【0005】

さらにまた、認証、暗号、および復号処理を、ワイアードロジックのハードウェアで実行させることも提案されている。

【0006】

【発明が解決しようとする課題】

しかしながら、ソフトウェアだけで認証処理、暗号化処理、および復号処理を行うようにする場合、ソフトウェアを解析し、改竄することで、音楽データが不正に複製されてしまう恐れがある。

【0007】

また、所定のIDをハードウェアに記憶させ、パーソナルコンピュータ上のソフトウェアにより、これを読み出し、利用させるようにする場合、読み出されたIDがソフトウェアに転送される途中において読み取られ、解析、改竄されてしまう

恐れがあった。

【0008】

さらに、認証処理、暗号化処理、および復号処理をワイアードロジックのハードウェアにより実行するようにすると、解析や改竄は防止することが可能であるが、新たな認証処理、暗号化処理、および復号処理を行うようにするには、既存のハードウェアを新たなハードウェアと交換するか、新たなハードウェアを追加する必要が生じる。

【0009】

本発明はこのような状況に鑑みてなされたものであり、記憶されているデータが不正に読み出され、解析されることを防止できるようにするものである。

【0010】

【課題を解決するための手段】

請求項1に記載の情報処理装置は、半導体ICに実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する通信手段と、認証局から受信した、暗号化されたプログラムを記録する記録手段と、記録手段に記録されているプログラムを、半導体ICに送信する送信手段とを含むことを特徴とする。

【0011】

請求項4に記載の情報処理方法は、半導体ICに実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する通信ステップと、認証局から受信した、暗号化されたプログラムを記録する記録ステップと、記録ステップで記録されているプログラムを、半導体ICに送信する送信ステップとを含むことを特徴とする情報処理方法。

【0012】

請求項5に記載の提供媒体は、情報処理装置に、半導体ICに実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する通信ステップと、認証局から受信した、暗号化されたプログラムを記録する記録ステップと、記録ステップで記録されているプログラムを、半導体ICに送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプ

プログラムを提供することを特徴とする。

【0013】

請求項6に記載の情報処理システムは、情報処理装置が、半導体ICに実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する通信手段と、認証局から受信した、暗号化されたプログラムを記録する記録手段と、記録手段に記録されているプログラムを、半導体ICに送信する送信手段とを含み、認証局が、半導体ICに実行させるプログラムを受信するとともに、情報処理装置に暗号化されたプログラムを送信する通信手段と、通信手段が受信したプログラムを所定の方式で暗号化する暗号化手段と含むことを特徴とする。

【0014】

請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載の提供媒体においては、半導体ICに実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ICに送信される。

【0015】

請求項6に記載の情報処理システムにおいては、半導体ICに実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ICに送信され、半導体ICに実行させるプログラムが受信されるとともに、情報処理装置に暗号化されたプログラムが送信され、受信したプログラムが所定の方式で暗号化される。

【0016】

【発明の実施の形態】

図1は、本発明を適用したネットワークシステムの構成例を表している。パーソナルコンピュータ1は、各種の処理を実行するCPU (Central Processing Unit) 12、各種のプログラムやデータを一時的に記憶するメモリ13、並びに、各種のプログラムやデータを大量に蓄積するハードディスク15を備えている。CD

-ROM (Read Only Memory) ドライブ 14 は、装着された CD-ROM に記録されているプログラムやデータを読み出す。IEC (International Electrotechnical Commission) 60958 端子 16a を有する音声入出力インタフェース 16 は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。インターネット接続インタフェース 11 は、インターネット 4 との間のインタフェース処理を実行する。インタフェース 17 は、アダプタ 3 またはメモリスティックウォークマン 2 との間のインタフェース処理、並びに、入力部 2 およびディスプレイ 3 に対するインタフェース処理を実行する。

【0017】

半導体 IC として、一体的に形成され、パーソナルコンピュータ 1 に装着されるアダプタ 3 の CPU 32 は、インタフェース 31 を介してパーソナルコンピュータ 1 の CPU 12 と共働し、各種の処理を実行する。RAM 33 は、CPU 32 が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ 34 は、パーソナルコンピュータ 1 の電源がオフされた後も保持する必要があるデータを記憶する。ROM 36 には、パーソナルコンピュータ 1 から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) 35 は、計時動作を実行し、時刻情報を提供する。

【0018】

メモリスティックウォークマン 2 は、不揮発性メモリ 23 を有し、パーソナルコンピュータ 1 からインタフェース 21 と認証装置 22 を介して提供されたデジタル音楽データを記憶する。認証装置 22 は、パーソナルコンピュータ 1 と不揮発性メモリ 23 との間でデータを授受するとき、相互に認証処理を実行する。インタフェース 21 は、パーソナルコンピュータ 1 との間のインタフェース処理、あるいは不揮発性メモリ 23 に記憶されている音楽データを読み出し、ヘッドホンなどを介してユーザに提供するためのインタフェース処理を実行する。

【0019】

パーソナルコンピュータ 1 は、インターネット 4 を介して EMD (Electrical Music Distribution) サーバ 5 と接続されており、EMD サーバ 5 から音楽データの

提供を受けることができる。

【0020】

次に、図2のフローチャートを参照して、CD-ROMドライブ14に装着されたCDから再生した音楽データをハードディスク15に転送し、コピーする場合の処理について説明する。ユーザが入力部2を操作して、インタフェース17を介してCPU12に対してCD-ROMドライブ14に装着されたCD（図示せず）から再生された音楽データをハードディスク15に転送、コピーする指令を入力すると、CPU12は、ステップS11において、インタフェース17を介してディスプレイ3にコピーする曲を選択するためのGUI（Graphical User Interface）を表示させる。

【0021】

具体的には、例えば、CPU12は、CD-ROMドライブ14に装着されたCDのTOC（Table Of Contents）を読み込み、そのCDに含まれる曲の情報を得て、ディスプレイ3に表示させる。または、CPU12は、CDに含まれている各曲毎のISRC（International Standard Recording Code）を読み出し、その曲の情報を得て、ディスプレイ3に表示させる。あるいはまた、CPU12は、インターネット4を介して外部のデータベースにアクセスし、TOCを用いて、そのCDの曲の情報を得て、対応するGUIをディスプレイ3に表示させる。ユーザは、ディスプレイ3のGUIを利用して入力部2を操作し、コピーする曲を選択する。

【0022】

次に、ステップS12において、CPU12は、ハードディスク15に記憶されている期限データベースをチェックする。この期限データベースチェック処理の詳細は、図3のフローチャートに示されている。

【0023】

ステップS31においてCPU12は、アダプタ7のCPU32と共働して、期限データベース全体のハッシュ値を計算し、ステップS32において、その計算された値と、前回保存しておいたハッシュ値と比較する。

【0024】

すなわち、ハードディスク15には、期限データベースが形成されており、こ

の期限データベースには、図4に示すように、ハードディスク15に記録されている音楽データを管理する管理情報として、過去に記録されたことのある曲のISRC番号とコピー日時が対応して記憶されている。この例においては、アイテム1乃至アイテム3の3つのアイテムについて、それぞれのISRCとコピー日時が記憶されている。この期限データベースに記録されている全ての曲のISRC番号とコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップS38において、アダプタ7のCPU32により計算され、不揮発性メモリ34に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。ハッシュ関数は、一般的に可変長の長いデータを、固定長の短い値にマップする一方向性の関数であり、ハッシュ値同士の衝突が起こりにくい性質を有している。ハッシュ関数の例としては、SHA、MD5などがある。CPU12は、ステップS31において、CPU32が実行したのと同様にハッシュ値を計算する。そして、ステップS32において、CPU12は、CPU32に、不揮発性メモリ34に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップS31で、いま自分自身が計算したハッシュ値とを比較する。

【0025】

ステップS33において、CPU12は、ステップS31でいま計算したハッシュ値と、不揮発性メモリ34に記憶されている前回の期限データベースのハッシュ値とが一致するか否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、CPU12は、ステップS34において、例えば、「期限データベースが改竄されたので、コピーができません」といったメッセージを発生し、インタフェース17を介してディスプレイ3に出力し、表示させ、以後、処理を終了させる。すなわち、この場合には、CDに記録されている音楽データを再生し、ハードディスク15にコピーする処理が禁止される。

【0026】

ステップS31で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップS35に進み、CPU12は、ステップS11で指定されたコピーする曲として選択された曲（選択曲）のISRC番号をCDから取得する。CDにISRC番号が記録されていない場合、CPU12は、そのCDのTOCのデータを読み出し、その

データにハッシュ関数を適用するなどして、例えば、58ビットなどの適当な長さのデータを得て、これをISRC番号に代えて用いる。

【0027】

ステップS36において、CPU12は、ステップS35で取得したISRC番号（すなわち、選択曲）が期限データベース（図4）に登録されているか否かを判定する。ISRC番号が期限データベースに登録されていない場合には、その曲はまだハードディスク15に登録されていないことになるので、ステップS37に進み、CPU12は、その曲のISRC番号と現在の日時とを期限データベースに登録する。なお、CPU12は、この現在の日時として、CPU32から転送を受けた、アダプタ7のRTC35が出力する値を利用する。そして、ステップS38において、CPU12は、その時点における期限データベースのデータを読み出し、アダプタ7のCPU32に転送する。CPU32は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ34に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップS32において、前回保存しておいたハッシュ値として利用される。

【0028】

次に、ステップS39において、CPU12は、選択曲が期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図2のステップS13において、選択曲が期限データベースに登録されているか否かの判定を行うときに用いられる。

【0029】

ステップS36において、選択曲のISRC番号が期限データベースに登録されていると判定された場合、その選択曲は、少なくとも一度、ハードディスク15に登録されたことがある曲であるということになる。そこで、この場合、ステップS40に進み、CPU12は、期限データベースに登録されているその選択曲の登録日時より、現在の日時（アダプタ7のRTC35が出力した現在の日時）が48時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に48時間以上経過している場合には、ハードディスク15に、少なくとも一度は記録したことがあるが、既に、その時から48時間以上経過しているので、その曲を

再度コピーさせたとしても、それほど実害がないので、この場合には、ハードディスク 15 へのコピーが許容される。そこで、ステップ S 4 1 に進み、CPU 1 2 は、期限データベースの日時を、過去の登録日時から現在の日時（RTC 3 5 の出力する日時）に変更させる。そして、ステップ S 3 8 に戻り、CPU 1 2 は、再び、期限データベース全体のハッシュ値を CPU 3 2 に計算させ、不揮発性メモリ 3 4 に保存させるとともに、ステップ S 3 9 において、その曲に対して未登録のフラグを設定する。

【0030】

一方、ステップ S 4 0 において、現在時刻が登録日時より、まだ 4 8 時間以上経過していないと判定された場合、その選択曲のハードディスク 15 へのコピーが禁止される。そこで、この場合には、ステップ S 4 2 に進み、CPU 1 2 は、その選択曲に対応して登録済みのフラグを設定する。

【0031】

以上のようにして、期限データベースチェック処理により、選択曲がハードディスク 15 に登録されているか否かを表すフラグが設定される。

【0032】

図 2 に戻り、ステップ S 1 3 において CPU 1 2 は、選択曲が期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択曲が登録済みである場合には、ステップ S 1 4 に進み、CPU 1 2 は、ディスプレイ 3 に、例えば、「この曲は一度コピーされてからまだ 4 8 時間以上経過していないので、コピーすることができません」のようなメッセージを表示させる。これにより、ユーザは、その曲をハードディスク 15 にコピーすることができない理由を知ることができる。

【0033】

ステップ S 1 3 において、選択した曲が期限データベースに登録されていないと判定された場合、ステップ S 1 5 に進み、CPU 1 2 は、CD-ROM ドライブ 1 4 を制御し、そこに装着されている CD から音楽データを読み出させる。この音楽データには、図 5 に示すように、所定の位置にウォーターマークコードが挿入されている。CPU 1 2 は、ステップ S 1 6 において、音楽データに含まれているウォーター

マークコードを抽出し、そのウォータマークコードがコピー禁止を表しているのか否かをステップ S 17 において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップ S 18 に進み、CPU 12 は、インタフェース 17 を介してディスプレイ 3 に、例えば、「コピーは禁止されています」のようなメッセージを表示させ、コピー処理を終了させる。

【0034】

これに対して、ステップ S 17 において、ウォータマークがコピー禁止を表していないと判定された場合、ステップ S 19 に進み、CPU 12 は、音楽データを、例えば、ATRAC (Adaptive Transform Acoustic Coding) (商標) などの方式で、ソフトウェア処理により圧縮させる。ステップ S 20 において、CPU 12 は、予め設定され、メモリ 13 に記憶されている暗号鍵を用いて、例えば、DES (Data Encryption Standard) 方式、FEAL (Fast Encipherment Algorithm) 方式などの暗号化方法により、音楽データを暗号化する。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ 7 の CPU 32 により発生させた乱数に基づいて生成したものをを用いることもできる。このように、パーソナルコンピュータ 1 だけではなく、それに付随して装着されたハードウェアとしてのアダプタ 7 の CPU 32 と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

【0035】

次に、ステップ S 21 において、CPU 12 は、暗号化されたデータをハードディスク 15 に転送し、1 つのファイルとしてファイル名を付けて保存させる。あるいはまた、1 つのファイルの一部として、そのファイル名の位置情報 (例えば、先頭からのバイト数) を与えて保存するようにしてもよい。

【0036】

この保存処理と、上記した圧縮符号化処理および暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

【0037】

さらに、ステップ S 22 において、CPU 12 は、予め定められているメモリ 13 に記憶されている保存用鍵を使って、上述した DES 方式、FEAL 方式などの方式

で、音楽データを暗号化した暗号鍵を暗号化し、ハードディスク 15 の曲データベースに保存する。

【0038】

ステップ S 23 において、CPU 12 は、保存したファイルに関する情報、暗号化された暗号鍵、その曲の情報、ユーザが GUI を介して入力した曲名の情報の要素を組にしてハードディスク 15 の曲データベースに登録する。そして、ステップ S 24 において、CPU 12 は、CPU 32 に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ 34 に保存させる。

【0039】

このようにして、例えば、図 6 に示すような曲データベースが、ハードディスク 15 上に登録される。この例においては、アイテム 1 乃至アイテム 3 のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ、およびコピー条件（SCMS）が記録されている。

【0040】

次に、図 7 乃至図 9 のフローチャートを参照して、ハードディスク 15 からメモリスティックウォークマン 6 の不揮発性メモリ 23（メモリスティック）に、音楽データを移動する処理について説明する。ステップ S 51 において、CPU 12 は、曲データベース全体のハッシュ値を計算し、ステップ S 52 で、前回 CPU 32 に計算させ、不揮発性メモリ 34 に保存しておいたハッシュ値と比較する。両者が一致しない場合、CPU 12 は、ステップ S 53 に進み、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ 3 に表示させた後、処理を終了させる。この場合の処理は、図 3 のステップ S 31 乃至ステップ S 34 の処理と同様の処理である。この場合においては、ハードディスク 15 からメモリスティックウォークマン 6 への音楽データの移動が実行されないことになる。

【0041】

次に、ステップ S 54 において、CPU 12 は、ハードディスク 15 に形成されている曲データベースから、そこに登録されている曲の情報を読み出し、ディス

プレイ 3 に、選択のための GUI として表示させる。ユーザは、この選択のための GUI に基づいて、ハードディスク 1 5 からメモリスティックウォークマン 6 へ移動させる曲を、入力部 2 を操作して選択する。次に、ステップ S 5 5 において、CPU 1 2 は、ステップ S 5 4 で選択された選択曲の再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図 1 0 のフローチャートを参照して後述する。

【0 0 4 2】

次に、ステップ S 5 6 において、パーソナルコンピュータ 1 の CPU 1 2 とメモリスティックウォークマン 6 の認証装置 2 2 との間において、相互認証処理が行われ、通信用鍵が共有される。

【0 0 4 3】

例えば、メモリスティックウォークマン 6 の不揮発性メモリ 2 3 には、マスター鍵 KM が予め記憶されており、パーソナルコンピュータ 1 のメモリ 1 3 には、個別鍵 K I と ID が予め記憶されているものとする。認証装置 2 2 は、CPU 1 2 から、メモリ 1 3 に予め記憶されている ID の供給を受け、その ID と自分自身が有するマスター鍵 KM にハッシュ関数（SHA などのハッシュ関数または DES などでも良い）を適用して、メモリ 1 3 に記憶されているパーソナルコンピュータ 1 の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ 1 とメモリスティックウォークマン 6 の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

【0 0 4 4】

あるいはまた、パーソナルコンピュータ 1 のメモリ 1 3 に ID とマスター鍵 K M P を予め記憶させておくとともに、メモリスティックウォークマン 6 の不揮発性メモリ 2 3 にもメモリスティックウォークマン 6 の ID とマスター鍵 K M M を記憶させておく。そして、それぞれの ID とマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきた ID とマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

【0045】

なお、認証の方法としては、例えば、IOS (International Organization for Standardization) 9798-2を利用することができる。

【0046】

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップS57において、CPU12は、選択曲のファイル名を曲データベースから読み出し、そのファイル名の音楽データ（例えば、図2のステップS20の処理で暗号化されている）をハードディスク15から読み出す。ステップS58において、CPU12は、ステップS57で読み出したデジタル音楽データの圧縮符号化方式（ステップS19の処理）、暗号化方式（ステップS20の処理）、フォーマットなどをメモリスティックウォークマン6のものに変換する処理を実行する。この変換処理の詳細は、図12のフローチャートを参照して後述する。

【0047】

ステップS59において、CPU12は、ステップS58で変換した音楽データを、ステップS56の相互認証処理により共有した通信用鍵で暗号化し、メモリスティックウォークマン6にインタフェース17を介して転送する。ステップS60において、メモリスティックウォークマン6の認証装置22は、インタフェース21を介してこの伝送されてきた音楽データを受信すると、その音楽データを、そのまま不揮発性メモリ23に記憶させる。

【0048】

ステップS61において、CPU12は、さらに、曲データベースに登録されているその選択曲の再生条件（開始日時、終了日時、回数制限など）を、メモリスティックウォークマン6が管理している形式に変換する。ステップS62において、CPU12は、さらに選択曲の曲データベース中に登録されているコピー条件中のSCMS情報を、メモリスティックウォークマン6の管理する形式に変換する。そして、ステップS63において、CPU12は、ステップS61で変換した再生条件と、ステップS62で変換したSCMS情報を、メモリスティックウォークマン6に転送する。メモリスティックウォークマン6の認証装置22は、転送を受け

た再生条件とSCMS情報を、不揮発性メモリ 23 に保存する。

【0049】

ステップ S 6 4 において、CPU 1 2 はまた、選択曲の曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU 1 2 が曲データベース中で扱っている形式のまま、メモリスティックウォークマン 6 に転送し、不揮発性メモリ 23 に保存させる。

【0050】

ステップ S 6 5 において、CPU 1 2 は、選択曲の暗号化されている暗号鍵を曲データベースから読み出し、ステップ S 6 6 において、その暗号鍵をメモリ 1 3 に保存されている保存用鍵で復号し、通信用鍵で暗号化する。そして、通信用鍵で暗号化した暗号鍵を、CPU 1 2 は、メモリスティックウォークマン 6 に転送する。

【0051】

メモリスティックウォークマン 6 の認証装置 2 2 は、ステップ S 6 7 で、パーソナルコンピュータ 1 から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、不揮発性メモリ 23 に保存する。

【0052】

認証装置 2 2 は、暗号鍵の保存が完了すると、ステップ S 6 8 において、パーソナルコンピュータ 1 に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ 1 の CPU 1 2 は、メモリスティックウォークマン 6 からこの通知を受けると、ステップ S 6 9 において、ハードディスク 1 5 から、その音楽データのファイルを削除するとともに、曲データベースからその曲の要素の組を削除する。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップ S 7 0 において、CPU 1 2 は、アダプタ 7 の CPU 3 2 に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ 3 4 に保存させる。このハッシュ値が、上述したステップ S 5 2 において、前回保存しておいたハッシュ値として用いられることになる。

【0053】

次に、図7のステップS55における選択曲の再生条件などのチェック処理について説明する。ステップS81において、CPU12は、曲データベースから、各種の条件を読み出す。CPU12は、ステップS82において、ステップS81で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既にすぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップS83に進み、CPU12は、例えば、「既にコピー回数がコピー制限回数に達しています」というようなメッセージをディスプレイ3に表示させ、処理を終了させる。ステップS82において、コピー回数がコピー制限回数を過ぎていないと判定された場合、ステップS84に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ7のRTC35より出力されたものが用いられる。これにより、ユーザが、パーソナルコンピュータ1の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。CPU12は、この現在日時をCPU32から提供を受けて、ステップS84の判断を自ら行うか、または、ステップS81で、曲データベースから読み出した再生条件をアダプタ7のCPU32に供給し、CPU32に、ステップS84の判定処理を実行させる。

【0054】

現在日時が再生終了日時を過ぎている場合、ステップS85に進み、CPU12は、選択曲をハードディスク15から消去するとともに、曲データベースから、その選択曲の情報を消去する。ステップS86において、CPU12は、CPU32に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ34に保存させる。以後、処理は終了される。従って、この場合、音楽データの移動が実行されない。

【0055】

ステップS84において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップS87に進み、CPU12は、その選択曲の再生時課金条件（例えば、再生1回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、CPU12は、ステップS88において、メモリスティックウォークマン6と通信し、メモリスティックウ

ウォークマン 6 に課金機能が存在するか否かを判定する。メモリスティックウォークマン 6 に課金機能が存在しない場合には、選択曲をメモリスティックウォークマン 6 に転送する訳にはいかないので、ステップ S 8 9 において、CPU 1 2 は、例えば、「転送先が課金機能を有していません」のようなメッセージをディスプレイ 3 に表示させ、音楽データの移動処理を終了させる。

【0056】

ステップ S 8 7 において再生時課金条件が登録されていないと判定された場合、または、ステップ S 8 8 において、メモリスティックウォークマン 6 に課金機能が存在すると判定された場合、ステップ S 9 0 に進み、CPU 1 2 は、選択曲に関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップ S 9 1 に進み、CPU 1 2 は、メモリスティックウォークマン 6 に、その再生条件を守る機能が存在するか否かを判定する。メモリスティックウォークマン 6 が、その再生条件を守る機能を有していない場合には、ステップ S 9 2 に進み、CPU 1 2 は、例えば、「転送先の装置が再生条件を守る機能を有していません」のようなメッセージをディスプレイ 3 に表示させ、処理を終了させる。

【0057】

ステップ S 9 0 において、再生条件が登録されていないと判定された場合、またはステップ S 9 1 において、メモリスティックウォークマン 6 が再生条件を守る機能を有している判定された場合、再生条件等のチェック処理が終了され、図 7 のステップ S 5 6 に戻る。

【0058】

図 11 は、メモリスティックウォークマン 6 が管理している（守ることが可能な）再生条件の例を表している。この例においては、アイテム 1 乃至アイテム 3 の各曲について、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム 2 についてのみ登録されており、アイテム 1 とアイテム 3 については登録されていない。従って、アイテム 2 の曲が選択曲とされた場合、再生回数の再生条件は守ることが可能であるが、アイテム 1 またはアイテム 3 の曲が選択曲とされた場合、再生回数の条件は守ることができないことになる。

【0059】

次に、図12のフローチャートを参照して、図7のステップS58におけるフォーマット変換処理の詳細について説明する。ステップS101において、CPU12は、ハードディスク15に記録されている選択曲のフォーマット（再生条件、使用条件、コピー条件など）を調べる。ステップS102において、CPU12は、相手先の機器（今の場合、メモリスティックウォークマン6）に設定することが可能な条件を調べる。すなわち、CPU12は、メモリスティックウォークマン6の認証装置22に設定可能な条件を問い合わせ、その回答を得る。ステップS103においてCPU12は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をステップS102で調べた条件に基づいて決定する。

【0060】

ステップS104において、CPU12は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップS105に進み、音楽データをメモリスティックウォークマン6に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をメモリスティックウォークマン6が守ることができないので、そのようなメモリスティックウォークマン6には、音楽データを移動することが禁止されるのである。

【0061】

ステップS104において設定可能な条件が存在すると判定された場合、ステップS106に進み、CPU12は、その条件を相手先の機能フォーマットの条件に変換する。そして、ステップS107において、変換した条件を相手先の機器に設定する。その結果、メモリスティックウォークマン6は、設定された条件に従って（その条件を守って）、音楽データ再生することが可能となる。

【0062】

次に、図13乃至図15のフローチャートを参照して、ハードディスク15からメモリスティックウォークマン6に音楽データをコピーする場合の処理について説明する。この図13乃至図15のステップS111乃至ステップS127の処理は、図7乃至図9のハードディスク15からメモリスティックウォークマン

6へ音楽データを移動させる場合のステップS51乃至ステップS67の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択曲の再生条件とのチェック処理が行われる。さらに、メモリスティックウォークマン6と、パーソナルコンピュータ1との間の相互認証処理の後、音楽データが、パーソナルコンピュータ1のハードディスク15からメモリスティックウォークマン6の不揮発性メモリ23に転送され、保存される。その後、ステップS128において、パーソナルコンピュータ1のCPU12は、曲データベースのコピー回数カウンタを1だけインクリメントする。そして、ステップS129において、CPU12は、CPU32に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ34に保存させる。

【0063】

次に、図16のフローチャートを参照して、メモリスティックウォークマン6からハードディスク15に音楽データを移動する処理について説明する。ステップS161において、パーソナルコンピュータ1のCPU12は、メモリスティックウォークマン6の認証装置22に対して不揮発性メモリ23に記憶されている曲の情報の読み出しを要求する。認証装置22は、この要求に対応して、不揮発性メモリ23に記憶されている曲の情報をパーソナルコンピュータ1に送信する。パーソナルコンピュータ1のCPU12は、この情報に基づいて、ディスプレイ3に、不揮発性メモリ23に記憶されている曲を選択するためのGUIを表示させる。ユーザは、入力部2を操作して、そのGUIに基づいて、メモリスティックウォークマン6からハードディスク15に移動させる曲を指定する。

【0064】

ステップS162において、CPU12は、認証装置22との間において、相互認証処理を実行し、通信用鍵を共有する。この処理は、図7のステップS56における場合と同様の処理である。

【0065】

次に、ステップS163において、認証装置22は、不揮発性メモリ23に記憶されている暗号化されている選択曲の音楽データを読み出し、パーソナルコンピュータ1に転送する。パーソナルコンピュータ1のCPU12は、ステップS1

64において、メモリスティックウォークマン6から転送されてきた音楽データを、1つのファイルとしてファイル名を付けて、ハードディスク15に保存する。この保存は、例えば、1つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

【0066】

ステップS165において、認証装置22は、不揮発性メモリ23に記憶されている選択曲の暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ1に転送する。この暗号鍵は、例えば、図9のステップS67の処理で不揮発性メモリ23に保存されていたものである。

【0067】

ステップS166において、パーソナルコンピュータ1のCPU12は、メモリスティックウォークマン6から暗号鍵の転送を受けると、それを通信用鍵で復号し、自分自身の保存用鍵で暗号化する。ステップS167で、CPU12は、ステップS164で保存した音楽データのファイルのファイル名、その曲の情報をユーザがGUIを介して入力した曲名、ステップS166で暗号化した暗号鍵などを、ハードディスク15の曲データベースに登録する。そして、ステップS168において、CPU12は、その曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させる。

【0068】

ステップS169において、パーソナルコンピュータ1のCPU12は、メモリスティックウォークマン6に対して暗号鍵が保存されたことを通知し、その曲の音楽データの削除を要求する。認証装置22は、パーソナルコンピュータ1から、その曲の音楽データの削除が要求されてきたとき、ステップS170において、不揮発性メモリ23に記憶されているその曲の音楽データを削除する。

【0069】

次に、メモリスティックウォークマン6からハードディスク15へ音楽データをコピーする場合の処理について、図17のフローチャートを参照して説明する。この図17に示すステップS181乃至ステップS188の処理は、図16の

メモリスティックウォークマン 6 からハードディスク 15 へ音楽データを移動させる場合の処理におけるステップ S 161 乃至ステップ S 168 の処理と同様の処理である。すなわち、コピー処理の場合は、図 16 のステップ S 169, S 170 の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

【0070】

次に、図 18 のフローチャートを参照して、EMD サーバ 5 から転送を受けた音楽データをハードディスク 15 にコピーする処理について説明する。ステップ S 201 において、CPU 12 は、入力部 2 を介してユーザから EMD サーバ 5 へのアクセスが指令されたとき、インターネット接続インタフェース 11 を制御し、インターネット 4 を介して EMD サーバ 5 にアクセスさせる。EMD サーバ 5 は、このアクセスに対応して、自分自身が保持している曲の曲番号、曲名、各情報などの情報を、インターネット 4 を介してパーソナルコンピュータ 1 に転送する。パーソナルコンピュータ 1 の CPU 12 は、インターネット接続インタフェース 11 を介して、この情報を取得したとき、それをインタフェース 17 を介してディスプレイ 3 に表示させる。ユーザは、ディスプレイ 3 に表示された GUI を利用して、ステップ S 202 において、コピーを希望する曲を指定する。この指定情報は、インターネット 4 を介して EMD サーバ 5 に転送される。ステップ S 203 において、CPU 12 は、EMD サーバ 5 との間において、インターネット 4 を介して相互認証処理を実行し、通信用鍵を共有する。

【0071】

パーソナルコンピュータ 1 と EMD サーバ 5 との間で行われる相互認証処理は、例えば、ISO 9798-3 で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ 1 は、自分自身の秘密鍵と EMD サーバ 5 の公開鍵を予め有しており、EMD サーバ 5 は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ 1 の公開鍵は、EMD サーバ 5 から転送したり、あるいはパーソナルコンピュータ 1 に予め配布されている certificate をパーソナルコンピュータ 1 から EMD サーバ 5 に転送し、その certificate を EMD サーバ 5 が確認し、公開鍵を得るようにしてもよい。さらに、ステッ

ブ S 2 0 4 において、CPU 1 2 は、EMDサーバ 5 との間において課金に関する処理を実行する。この課金の処理の詳細は、図 1 9 のフローチャートを参照して後述する。

【0072】

次に、ステップ S 2 0 5 において、EMDサーバ 5 は、パーソナルコンピュータ 1 に対して、ステップ S 2 0 2 で指定された曲の暗号化されている音楽データをインターネット 4 を介してパーソナルコンピュータ 1 に転送する。このとき、時刻情報も適宜転送される。ステップ S 2 0 6 において、CPU 1 2 は、転送を受けた音楽データをファイル名を付けてハードディスク 1 5 に 1 つのファイルとして保存する。ステップ S 2 0 7 において、EMDサーバ 5 は、さらに、その曲の暗号鍵をステップ S 2 0 3 でパーソナルコンピュータ 1 と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ 1 へ転送する。

【0073】

CPU 1 2 は、ステップ S 2 0 8 において、EMDサーバ 5 より転送を受けた暗号鍵を単独で、またはアダプタ 7 の CPU 3 2 と共同して通信用鍵を用いて復号し、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化する。ステップ S 2 0 9 において、CPU 1 2 は、その曲のファイル名、曲の情報、ユーザが入力した曲名、暗号化された暗号鍵を組にして、ハードディスク 1 5 の曲データベースに登録する。さらに、ステップ S 2 1 0 において、CPU 1 2 は、その曲データベース全体のハッシュ値を CPU 3 2 に計算させ、不揮発性メモリ 3 4 に保存させる。

【0074】

なお、ステップ S 2 0 5 において EMDサーバ 5 は、音楽データとともに、時刻データをパーソナルコンピュータ 1 に送信する。この時刻データは、パーソナルコンピュータ 1 からアダプタ 7 に転送される。アダプタ 7 の CPU 3 2 は、パーソナルコンピュータ 1 より転送されてきた時刻データを受信すると、ステップ S 2 1 1 において、RTC 3 5 の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ 7 の RTC 3 5 の時刻情報を修正するようにしたので、アダプタ 7 を常に正しい時刻情報を保持することが可能となる。

【0075】

また、RTC35を利用する処理を、後述する暗号化されたソースプログラムまたはオブジェクトプログラムでのみ実行させるようにすれば、時刻情報の改竄が困難になる。

【0076】

次に、図19のフローチャートを参照して、図18のステップS204における課金に関する処理の詳細について説明する。ステップS221において、パーソナルコンピュータ1のCPU12は、ステップS201でEMDサーバ5から伝送されてきた価格情報の中から、ステップS202で指定された選択曲の価格情報を読み取り、これをハードディスク15上の課金ログに書き込む。図20は、このような課金ログの例を表している。この例においては、ユーザは、アイテム1乃至アイテム3を、EMDサーバ5からコピーしており、アイテム1とアイテム2の領域は50円とされ、アイテム3の料金は60円とされている。その時点における課金ログのハッシュ値も、CPU32により計算され、不揮発性メモリ34に登録されている。

【0077】

次に、ステップS222において、パーソナルコンピュータ1のCPU12は、ステップS221で書き込んだ課金ログをハードディスク15から読み出し、これをインターネット4を介してEMDサーバ5に転送する。EMDサーバ5は、ステップS223において、パーソナルコンピュータ1から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、EMDサーバ5は、内蔵するデータベースに、パーソナルコンピュータ1のユーザから伝送されてきた課金ログを追加更新する。そして、ステップS224において、EMDサーバ5は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップS225に進み、EMDサーバ5は、決裁に必要な商品名、金額などを決裁サーバ（図示せず）に転送する。そして、ステップS226において、決裁サーバは、パーソナルコンピュータ1のユーザに対する決裁処理を実行する。ステップS224において、決裁は直ちには行われないと判定された場合、ステップS225とS226の処理はスキップされる。すなわち、この処理は、例えば、月に1回など

、定期的にその後実行される。

【0078】

次に、図21と図22のフローチャートを参照して、音声入出力インタフェース16のIEC60958端子16aから入力された、図示せぬCDプレーヤなどからの再生音楽データを、ハードディスク15にコピーする場合の処理について説明する。ステップS241において、ユーザは、CDプレーヤのIEC60958出力端子を、パーソナルコンピュータ1の音声入出力インタフェース16のIEC60958端子16aに接続する。ステップS242において、ユーザは、入力部2を操作し、CDプレーヤからコピーする曲の曲名を入力する。そして、ステップS243においてユーザは、CDプレーヤのボタンを操作し、CDプレーヤの再生を開始させる。CDプレーヤとパーソナルコンピュータ1との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ1の入力部2を介して再生開始指令を入力することで、CDプレーヤにCDの再生を開始させることも可能である。

【0079】

CDプレーヤにおいて、CDの再生が開始されると、ステップS244において、CDプレーヤから出力された音楽データが、IEC60958端子16aを介してパーソナルコンピュータ1に転送されてくる。ステップS245において、CPU12は、IEC60958端子16aを介して入力されてくるデータから、SCMS (Serial Copy Management System) データを読み取る。このSCMSデータには、コピー禁止、コピー1回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップS246において、CPU12は、SCMSデータがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップS247に進み、CPU12は、ディスプレイ3に、例えば、「コピーが禁止されています」といったメッセージを表示させ、コピー処理を終了する。すなわち、この場合には、ハードディスク15へのコピーが禁止される。

【0080】

CPU12は、ステップS246において、ステップS245で読み取ったSCMS情報がコピー禁止を表していないと判定した場合、ステップS248に進み、ウ

ウォーターマークコードを読み出し、そのウォーターマークがコピー禁止を表しているか否かをステップ S 2 4 9 において判定する。ウォーターマークコードがコピー禁止を表している場合には、ステップ S 2 4 7 に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

【 0 0 8 1 】

ステップ S 2 4 9 において、ウォーターマークがコピー禁止を表していないと判定された場合、ステップ S 2 5 0 に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択曲が既に登録されていれば、ステップ S 2 5 1, S 2 5 2 の処理で、処理が終了される。この処理は、図 2 のステップ S 1 3, S 1 4 の処理と同様の処理である。

【 0 0 8 2 】

選択曲がまだハードディスク 1 5 に登録されていない曲であれば、ステップ S 2 5 3 乃至 S 2 5 8 で、その登録処理が実行される。このステップ S 2 5 3 乃至ステップ S 2 5 8 の処理は、ステップ S 2 5 7 において、IEC 6 0 9 5 8 端子から供給されてくる SCMS 情報も曲データベースに登録される点を除き、図 2 のステップ S 1 9 乃至ステップ S 2 4 の処理と同様の処理であるので、その説明は省略する。

【 0 0 8 3 】

次に、図 2 3 と図 2 4 のフローチャートを参照して、音楽データをハードディスク 1 5 から IEC 6 0 9 5 8 端子 1 6 a に出力（再生）する場合の処理について説明する。ステップ S 2 7 1 乃至ステップ S 2 7 3 において、図 1 3 のステップ S 1 1 1 乃至 S 1 1 3 における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップ S 2 7 4 に進み、CPU 1 2 は、ハードディスク 1 5 の曲データベースにアクセスし、そこに登録されている曲の情報を読み出し、ディスプレイ 3 に表示させる。ユーザは、その表示を見て、入力部 2 を適宜操作して、再生出力する曲を選択する。ステップ S 2 7 5 において、CPU 1 2 は、選択曲の再生条件等のチェック処理を実行する。この再生条件等のチェック処

理の詳細は、図25のフローチャートを参照して後述する。

【0084】

次に、ステップS276において、CPU12は、ステップS274において選択された曲の暗号鍵を曲データベースから読み出し、保存用鍵で復号する。ステップS277において、CPU12は、選択曲のSCMS情報を曲データベースから読み出し、IEC60958端子から出力するSCMS情報を、SCMSシステムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は1だけインクリメントされ、新たなSCMS情報とされる。ステップS278において、CPU12はさらに、選択曲のISRCを曲データベースから読み出す。

【0085】

次に、ステップS279において、CPU12は、曲データベースから選択曲ファイル名を読み出し、そのファイル名を基に、その音楽データをハードディスク15から読み出す。CPU12はさらに、その音楽データに対応する暗号鍵を曲データベースから読み出し、保存用鍵で復号し、復号した暗号鍵を用いて、暗号化されている音楽データを復号する。CPU12は、さらに、その音楽データの圧縮符号を復号する。ステップS280において、CPU12は、ステップS279で、復号したデジタル音楽データを、ステップS277で決定したSCMS情報、並びにステップS278で読み出したISRC情報とともに、IEC60958の規定に従って、IEC90958端子16aから出力する。さらにまた、デジタル音楽データをアナログ化し、音声入出力インタフェース16のアナログ出力端子から出力する。

【0086】

ステップS281において、CPU12は、曲データベース中の再生回数カウンタの値を1だけインクリメントする。そして、ステップS282において、選択曲に再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS283に進み、CPU12は、対応する料金を課金ログに書き込み、ステップS284において、曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に記憶させる。ステップS282において、選択曲に再生時課金条件が付加されていないと判定された場合、ステ

ップ S 2 8 3 とステップ S 2 8 4 の処理はスキップされる。

【0087】

次に、図 2 5 のフローチャートを参照して、図 2 3 のステップ S 2 7 5 の再生条件等のチェック処理の詳細について説明する。ステップ S 3 0 1 において、CPU 1 2 は、曲データベースの各種条件を読み出す。ステップ S 3 0 2 において CPU 1 2 は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップ S 3 0 3 に進み、選択曲をハードディスク 1 5 から削除させるとともに、曲データベースから選択曲の情報を削除させる。ステップ S 3 0 4 において、CPU 1 2 はさらに、曲データベースの新たなハッシュ値を CPU 3 2 に計算させ、そのハッシュ値を不揮発性メモリ 3 4 に保存させる。この場合、再生出力は禁止される。

【0088】

ステップ S 3 0 2 において、再生回数が制限回数を過ぎていないと判定された場合、ステップ S 3 0 5 に進み、CPU 1 2 は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した場合と同様にステップ S 3 0 3 において、選択曲をハードディスクから削除させるとともに、曲データベースからも削除させる。そして、ステップ S 3 0 4 において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

【0089】

ステップ S 3 0 5 において、再生終了日時が現在日時を過ぎていないと判定された場合は、ステップ S 3 0 6 に進み、CPU 3 2 は、その選択曲に対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップ S 3 0 7 に進み、CPU 1 2 は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ 3 に表示させる。ステップ S 3 0 6 において、再生時課金条件が付加されていないと判定された場合、ステップ S 3 0 7 の処理はスキップされる。

【0090】

次に、図 2 6 と図 2 7 のフローチャートを参照して、ハードディスク 1 5 から

メモリスティックウォークマン 6 経由で音楽データを出力（再生）する場合の処理について説明する。ステップ S 3 2 1 乃至ステップ S 3 2 5 において、曲データベースの改竄チェックと選択曲の指定、並びに選択曲の再生条件等のチェック処理が行われる。その処理は、図 2 3 のステップ S 2 7 1 乃至ステップ S 2 7 5 の処理と同様の処理であるので、その説明は省略する。

【0091】

ステップ S 3 2 6 において、メモリスティックウォークマン 6 とパーソナルコンピュータ 1 の間で相互認証処理が実行され、相互の間で、通信用鍵が共有される。ステップ S 3 2 7 において、パーソナルコンピュータ 1 の CPU 1 2 は、メモリスティックウォークマン 6 に対して、これから送る暗号化音声データを再生するように命令する。ステップ S 3 2 8 において、CPU 1 2 は、ステップ S 3 2 4 で指定された選択曲のファイル名を曲データベースから読み出し、そのファイル名の音楽データをハードディスク 1 5 から読み出す。CPU 1 2 は、ステップ S 3 2 9 において、音楽データの圧縮符号化方式、暗号化方式、フォーマットなどをメモリスティックウォークマン 6 の方式のものに変換する処理を実行する。そして、ステップ S 3 3 0 において、CPU 1 2 は、ステップ S 3 2 9 において変換した音楽データを通信用鍵で暗号化し、メモリスティックウォークマン 6 に転送する。

【0092】

ステップ S 3 3 1 において、メモリスティックウォークマン 6 の認証装置 2 2 は、ステップ S 3 2 7 において、パーソナルコンピュータ 1 から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップ S 3 3 2 において、CPU 1 2 は、曲データベースの再生回数カウンタを 1 だけインクリメントする。さらに、ステップ S 3 3 3 において、CPU 1 2 は、選択曲に再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップ S 3 3 4 において、その料金を課金ログに書き込み、ステップ S 3 3 5 において、CPU 3 2 に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択曲に再生時課金条件が付加されていない場合には、ステップ S 3 3 4、ステップ S 3 3 5 の処理はスキップされる。

【0093】

本発明においては、音楽データが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU 1 2 を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

【0094】

さらに、上述したように、CPU 1 2 の機能の一部は、ハードウェアとしてのアダプタ 7 に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高めることが可能となっている。

【0095】

例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるのではなく、アダプタ 7 の不揮発性メモリ 3 4 に保存される。すなわち、図 3 のステップ S 3 2, S 3 3 などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ 3 4 に記憶されているものとされる。これにより、例えば、ハードディスク 1 5 に保存されている音楽データを、他の記録媒体にコピーまたは移動させる前に、ハードディスク 1 5 の記録内容をバックアップしておき、ハードディスク 1 5 から、そこに保存されている音楽データを他の記録媒体にコピーまたはムーブした後、ハードディスク 1 5 にバックアップしておいたデータを再びリストアすることで、実質的に再現なく、コピーまたはムーブができてしまうようなことが防止される。

【0096】

例えば、図 2 8 に示すように、ハードディスク 1 5 に曲 A, B が保存されている場合、不揮発性メモリ 3 4 には、曲 A と曲 B の情報に対応するハッシュ値が保存されている。この状態において、ハードディスク 1 5 の記録データを他の記録媒体 5 1 にバックアップしたとする。その後、ハードディスク 1 5 に保存されている曲 A と曲 B のうち、曲 A を他の記録媒体 5 2 に移動させた場合、その時点において、ハードディスク 1 5 に記録されている曲は、曲 B だけとなるので、不揮発性メモリ 3 4 のハッシュ値も、曲 B に対応するハッシュ値に変更される。

【0097】

従って、その後、記録媒体51にバックアップしておいたハードディスク15の内容をハードディスク15にリストアして、ハードディスク15に、再び曲Aと曲Bを保存させたとしても、不揮発性メモリ34には、曲Bの情報から演算されたハッシュ値が記憶されており、曲Aと曲Bの情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、ハードディスク15に記憶されている曲Aと曲Bに基づくハッシュ値が、不揮発性メモリ34に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、ハードディスク15に保存されている曲Aと曲Bの利用が制限されてしまうことになる。

【0098】

さらに、上述したように、アダプタ7は、RTC35を内蔵しており、このRTC35の値は、正しい認証結果が得られた他の装置（例えば、EMDサーバ5）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ1が管理するものではなく、RTC35が出力するものが利用される。従って、ユーザが、パーソナルコンピュータ1の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

【0099】

また、アダプタ7は、暗号化されて転送されてきたプログラムをROM36に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図29のフローチャートを参照して説明する。

【0100】

すなわち、パーソナルコンピュータ1は、アダプタ7に対して、所定の処理を実行させたいとき、ステップS351において、アダプタ7に実行させるべきプログラムをメモリ13に予め記憶されている暗号鍵を用いて暗号化してアダプタ7に転送する。アダプタ7のROM36には、パーソナルコンピュータ1から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラム

が予め記憶されている。CPU 32は、このROM 36に記憶されているプログラムに従って、パーソナルコンピュータ1から転送されてきた暗号化されているプログラムをステップS 352において復号する。そして、ステップS 313において、CPU 32は、復号したプログラムをRAM 33に展開し、ステップS 354において、そのプログラムを実行する。

【0101】

例えば、上述したように、パーソナルコンピュータ1のCPU 12は、ハードディスク15の曲データベースのハッシュ値をアダプタ7に計算させるとき、曲データベースのデータを暗号鍵で暗号化してアダプタ7のCPU 32に転送する。CPU 32は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ34に記憶させる。あるいは、そのハッシュ値を、CPU 32は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ1のCPU 12に転送する。

【0102】

図30は、アダプタ7の内部のより具体的な構成を表している。アダプタ7は、半導体ICとして形成される。アダプタ7は、図1に示したインタフェース31、CPU 32、RAM 33、不揮発性メモリ34、RTC 35、ROM 36以外に、RAM 33に対する書き込みと読み出しを制御するRAMコントローラ61、並びに論理回路62を有している。論理回路62は、例えば、暗号化されている音楽データを解読した後、解読したデータをアダプタ7から直接出力するような場合の処理のために用いられる。

【0103】

これらのインタフェース31乃至ROM 36、RAMコントローラ61、並びに論理回路62は、半導体IC内に一体的に組み込まれ、外部からは分解できないように構成されている。

【0104】

水晶振動子71は、アダプタ7が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路72は、RTC 35を動作させる

ための発振回路である。バッテリー 73 は、発振回路 72、不揮発性メモリ 34、および RTC 35 に対してバックアップ用の電力を供給している。アダプタ 7 のその他の回路には、パーソナルコンピュータ 1 の電源供給回路 81 からの電力が供給されている。

【0105】

不揮発性メモリ 34 は、書き込み消去可能な ROM で構成することも可能であるが、バッテリー 73 からのバックアップ電源でバックアップされる RAM で構成する場合には、例えば、図 31 に示すように、不揮発性メモリ 34 の上に保護アルミニウム層 91 を形成し、さらに、その保護アルミニウム層 91 と同一平面上となるように、不揮発性メモリ 34 にバッテリー 73 からの電力を供給する電源パターン 92 を形成するようにすることができる。このようにすると、例えば、不揮発性メモリ 34 を改竄すべく、保護アルミニウム層 91 を削除しようとする、同一平面上の電源パターン 92 も削除されてしまい、不揮発性メモリ 34 に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

【0106】

さらに、図 32 に示すように、不揮発性メモリ 34 に対するデータの書き込みまたは読み出しのための配線 101-1 乃至 101-3 は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線 101-3 からデータを読み出すためには、上方の配線 101-1、101-2 を除去しなければならず、複数の配線 101-1、101-2、101-3 から同時にデータを読み取ることができなくなる。さらにまた、この配線 101-1 乃至 101-3 を冗長に形成し、直接プローブすると、その付加容量により、その内容を解析することが困難になるようにすることができる。

【0107】

次に、メモリスティックウォークマン 6 がパーソナルコンピュータ 1 から所定のデータを受け取る場合の、相互認証の処理を図 33 および図 34 のフローチャートを参照して説明する。ステップ S401 において、パーソナルコンピュータ

1のCPU12は、乱数Naを生成する。ステップS402において、パーソナルコンピュータ1のCPU12は、インターフェース17に、パーソナルコンピュータ1のID、鍵のカテゴリ番号G、および乱数Naをメモリスティックワークマン6へ送信させる。

【0108】

ステップS421において、メモリスティックワークマン6の認証装置22は、乱数Nbを生成する。ステップS422において、メモリスティックワークマン6は、インターフェース31を介して、パーソナルコンピュータ1から送信されたパーソナルコンピュータ1のID、鍵のカテゴリ番号G、および乱数Naを受信する。ステップS423において、メモリスティックワークマン6の認証装置22は、鍵のカテゴリ番号Gから、マスター鍵KMaの鍵番号jを求める。

【0109】

ステップS424において、メモリスティックワークマン6の認証装置22は、j番目のマスター鍵KMa[j]を求める。ステップS425において、メモリスティックワークマン6の認証装置22は、パーソナルコンピュータ1のIDに、マスター鍵KMa[j]を基にしたSHAなどのハッシュ関数を適用し、鍵Kabを求める。

【0110】

ステップS426において、メモリスティックワークマン6の認証装置22は、乱数Na、乱数Nb、およびパーソナルコンピュータ1のIDに、鍵Kabを基にしたSHAなどのハッシュ関数を適用し、乱数R1を求める。ステップS427において、メモリスティックワークマン6の認証装置22は、乱数Sbを生成する。

【0111】

ステップS428において、メモリスティックワークマン6の認証装置22は、インターフェース31に、乱数Na、乱数Nb、鍵番号j、および乱数Sbをパーソナルコンピュータ1へ送信させる。

【0112】

ステップS403において、パーソナルコンピュータ1は、インターフェース17を介して、乱数Na、乱数Nb、鍵番号j、および乱数Sbを受信する。ステップS404において、パーソナルコンピュータ1のCPU12は、鍵番号jを基に、個別鍵KIaに含まれる鍵Kabを求める。ステップS405において、パーソナルコンピュータ1のCPU12は、乱数Na、乱数Nb、およびパーソナルコンピュータ1のIDに、鍵Kabを基にしたSHAなどのハッシュ関数を適用し、乱数R2を求める。

【0113】

ステップS406において、パーソナルコンピュータ1のCPU12は、受信した乱数R1と、ステップS405で生成した乱数R2とが等しいか否かを判定し、乱数R1と乱数R2とが等しくないと判定された場合、正当なメモリスティックウォークマンではないので、メモリスティックウォークマン6を認証せず、処理は終了する。ステップS406において、乱数R1と乱数R2とが等しいと判定された場合、メモリスティックウォークマン6は正当なメモリスティックウォークマンなので、ステップS407に進み、パーソナルコンピュータ1のCPU12は、乱数Saを生成する。

【0114】

ステップS408において、パーソナルコンピュータ1のCPU12は、乱数Nbおよび乱数Naに、鍵Kabを基にしたSHAなどのハッシュ関数を適用し、乱数R3を求める。ステップS409において、パーソナルコンピュータ1のCPU12は、インターフェース17に、乱数R3および乱数Sbをメモリスティックウォークマン6へ送信させる。ステップS410において、パーソナルコンピュータ1のCPU12は、乱数Saおよび乱数Sbに、鍵Kabを基にしたSHAなどのハッシュ関数を適用し、一時鍵Ksを求める。

【0115】

ステップS429において、メモリスティックウォークマン6の認証装置22は、インターフェース31を介して、乱数R3および乱数Sbを受信する。ステップS430において、メモリスティックウォークマン6の認証装置22は、乱数Nbおよび乱数Naに、鍵Kabを基にしたSHAなどのハッシュ関数を適用

し、乱数R4を求める。ステップS431において、メモリスティックウォークマン6の認証装置22は、受信した乱数R3と、ステップS430で生成した乱数R4とが等しいか否かを判定し、乱数R3と乱数R4とが等しくないと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ1を認証せず、処理は終了する。ステップS431において、乱数R3と乱数R4とが等しいと判定された場合、パーソナルコンピュータ1は正当なパーソナルコンピュータなので、ステップS432に進み、メモリスティックウォークマン6の認証装置22は、乱数Saおよび乱数Sbに、鍵Kabを基にしたSHAなどのハッシュ関数を適用し、一時鍵Ksを求める。

【0116】

以上のように、パーソナルコンピュータ1およびメモリスティックウォークマン6は、相互認証し、共通の一時鍵Ksを得る。なお、ステップS425、ステップS426、ステップS405、ステップS408、ステップS410、ステップS430、およびステップS432において、SHAなどのハッシュ関数を適用するとして説明したが、DESなどを適用しても良い。

【0117】

次に、パーソナルコンピュータ1がメモリスティックウォークマン6に所定のデータを送信する場合の、相互認証の処理を図34および図36のフローチャートを参照して説明する。ステップS451において、パーソナルコンピュータ1のCPU12は、乱数Naを生成する。ステップS452において、パーソナルコンピュータ1は、インターフェース17を介して、パーソナルコンピュータ1のID、パーソナルコンピュータ1の鍵のカテゴリ番号Gp、メモリスティックウォークマン6の鍵のカテゴリ番号Gs、および乱数Naをメモリスティックウォークマン6に送信する。

【0118】

ステップS481において、メモリスティックウォークマン6の認証装置22は、乱数Nbを生成する。ステップS482において、メモリスティックウォークマン6は、インターフェース31を介して、パーソナルコンピュータ1から送信されたパーソナルコンピュータ1のID、パーソナルコンピュータ1の鍵のカテ

ゴリ番号 G_p 、メモリスティックウォークマン 6 の鍵のカテゴリ番号 G_s 、および乱数 N_a を受信する。ステップ S 483 において、メモリスティックウォークマン 6 の認証装置 22 は、メモリスティックウォークマン 6 の鍵のカテゴリ番号 G_s から、マスター鍵 KMa の鍵番号 j を求める。

【0119】

ステップ S 484 において、メモリスティックウォークマン 6 の認証装置 22 は、 j 番目のマスター鍵 $KMa[j]$ を求める。ステップ S 485 において、メモリスティックウォークマン 6 の認証装置 22 は、パーソナルコンピュータ 1 の ID に、マスター鍵 $KMa[j]$ を基にした SHA などのハッシュ関数を適用ハッシュ関数を適用し、鍵 Kab を求める。ステップ S 486 において、メモリスティックウォークマン 6 の認証装置 22 は、パーソナルコンピュータ 1 の鍵のカテゴリ番号 G_p を基に、マスター鍵 KIa の鍵番号 k を求める。ステップ S 487 において、メモリスティックウォークマン 6 の認証装置 22 は、鍵 Kab に、マスター鍵 $KIa[k]$ を基にした SHA などのハッシュ関数を適用ハッシュ関数を適用し、鍵 $K'ab$ を求める。

【0120】

ステップ S 488 において、メモリスティックウォークマン 6 の認証装置 22 は、乱数 N_a および乱数 N_b に、鍵 $K'ab$ を基にした SHA などのハッシュ関数を適用ハッシュ関数を適用し、乱数 R_1 を求める。ステップ S 489 において、メモリスティックウォークマン 6 の認証装置 22 は、乱数 S_b を生成する。

【0121】

ステップ S 490 において、メモリスティックウォークマン 6 の認証装置 22 は、インターフェース 31 に、メモリスティックウォークマン 6 の ID、乱数 N_b 、乱数 R_1 、鍵番号 j 、および乱数 S_b をパーソナルコンピュータ 1 へ送信させる。

【0122】

ステップ S 453 において、パーソナルコンピュータ 1 は、インターフェース 17 を介して、メモリスティックウォークマン 6 の ID、乱数 N_b 、乱数 R_1 、鍵番号 j 、および乱数 S_b を受信する。ステップ S 454 において、パーソナルコ

ンピュータ1のCPU12は、メモリスティックウォークマン6のIDに、パーソナルコンピュータ1のマスター鍵KMPを基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、マスター鍵Kmを求める。ステップS455において、パーソナルコンピュータ1のCPU12は、j番目の個別鍵KIaを求める。ステップS456において、パーソナルコンピュータ1のCPU12は、乱数Naおよび乱数Nbに、鍵KIaを基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、鍵K'abを求める。ステップS457において、パーソナルコンピュータ1のCPU12は、乱数Naおよび乱数Nbに、鍵K'abを基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、乱数R2を求める。

【0123】

ステップS458において、パーソナルコンピュータ1のCPU12は、受信した乱数R1と、ステップS457で生成した乱数R2とが等しいか否かを判定し、乱数R1と乱数R2とが等しくないと判定された場合、正当なメモリスティックウォークマンではないので、メモリスティックウォークマン6を認証せず、処理は終了する。ステップS458において、乱数R1と乱数R2とが等しいと判定された場合、メモリスティックウォークマン6は正当なメモリスティックウォークマンなので、ステップS459に進み、パーソナルコンピュータ1のCPU12は、乱数Saを生成する。

【0124】

ステップS460において、パーソナルコンピュータ1のCPU12は、乱数Nbおよび乱数Naに、鍵KIaを基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、乱数R3を求める。ステップS461において、パーソナルコンピュータ1のCPU12は、インターフェース17を介して、メモリスティックウォークマン6に、乱数R3および乱数Sbを送信する。ステップS462において、パーソナルコンピュータ1のCPU12は、乱数Saおよび乱数Sbに、鍵K'abを基にしたSHAなどのハッシュ関数を適用ハッシュ関数を適用し、一時鍵Ksを求める。

【0125】

ステップS491において、メモリスティックウォークマン6の認証装置22は、インターフェース31を介して、乱数R3および乱数Sbを受信する。ステップS492において、メモリスティックウォークマン6の認証装置22は、乱数Nbおよび乱数Naに、鍵Kabを基にしたSHAなどのハッシュ関数を適用し、乱数R4を求める。ステップS493において、メモリスティックウォークマン6の認証装置22は、受信した乱数R3と、ステップS492で生成した乱数R4とが等しいか否かを判定し、乱数R3と乱数R4とが等しくないとは判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ1を認証せず、処理は終了する。ステップS493において、乱数R3と乱数R4とが等しいとは判定された場合、パーソナルコンピュータ1は、正当なパーソナルコンピュータなので、ステップS494に進み、メモリスティックウォークマン6の認証装置22は、乱数Saおよび乱数Sbに、鍵Kabを基にしたSHAなどのハッシュ関数を適用し、一時鍵Ksを求める。

【0126】

このように、パーソナルコンピュータ1およびメモリスティックウォークマン6は、相互認証し、共通の一時鍵Ksを得る。図35および図36のフローチャートに示した手続きは、図33および図34のフローチャートに示す手続きよりも、いわゆる”なりすまし”に対する防御（検出）が強力である。なお、ステップS485、ステップS487、ステップS488、ステップS454、ステップS456、ステップS457、ステップS460、ステップS462、ステップS492、およびステップS494において、SHAなどのハッシュ関数を適用するとして説明したが、DESなどを適用しても良い。

【0127】

以上のように、パーソナルコンピュータ1およびメモリスティックウォークマン6は、相互認証の後に行われる処理に対応し、検出力が異なる相互認証の手続きを使い分けることにより、効率的かつ強力に、なりすましによる攻撃に対応することができる。

【0128】

次に、ソースプログラムを暗号化する処理を、図37のフローチャートを参照して説明する。ステップS501において、パーソナルコンピュータ1は、インターネット接続インターフェース11を介して、図示せぬ認証局に署名を付したソースプログラムを送信する。ステップS502において、認証局は、署名を基に、受信したソースプログラムに改竄が発見されたか否かを判定し、受信したソースプログラムに改竄が発見された場合、処理は継続できないので、処理は終了する。

【0129】

ステップS502において、受信したソースプログラムに改竄が発見されなかった場合、ステップS503に進み、認証局は、受信したソースプログラムを認証局の秘密鍵で暗号化する。ステップS504において、認証局は、暗号化したソースプログラムをパーソナルコンピュータ1に送信する。ステップS505において、パーソナルコンピュータ1は、受信したソースプログラムを、ハードディスク15に記録し、処理は終了する。

【0130】

以上のように、ソースプログラムは、暗号化される。なお、認証局に代わり、EDMサーバ5または所定の安全なサーバが、ソースプログラムを暗号化するようにしてもよい。

【0131】

次に、暗号化されたソースプログラムをアダプタ7が実行する処理を、図38のフローチャートを参照して説明する。ステップS521において、アダプタ7のCPU32は、パーソナルコンピュータ1から受信した、暗号化されたソースプログラムを、不揮発性メモリ34に予め記憶されている認証局の公開鍵で復号する。ステップS522において、アダプタ7のCPU32は、インタープリタを起動し、復号されたソースプログラムを実行する。

【0132】

ステップS523において、アダプタ7のCPU32は、ソースプログラムを実行して得られた結果を、パーソナルコンピュータ1に送信するか否かを判定し、結果をパーソナルコンピュータ1に送信しないと判定された場合、処理は終了

する。ステップ S 5 2 3 において、結果をパーソナルコンピュータ 1 に送信すると判定された場合、ステップ S 5 2 4 に進み、アダプタ 7 の CPU 3 2 は、ソースプログラムを実行して得られた結果を所定の鍵で暗号化する。ステップ S 5 2 5 において、アダプタ 7 の CPU 3 2 は、インターフェース 3 1 を介して、暗号化された結果をパーソナルコンピュータ 1 に送信し、処理は終了する。

【 0 1 3 3 】

以上のように、アダプタ 7 は、暗号化されたソースプログラムを実行し、所定の場合、得られた結果を暗号化し、パーソナルコンピュータ 1 に送信する。

【 0 1 3 4 】

なお、オブジェクトプログラムを暗号化し、暗号化されたオブジェクトプログラムをアダプタ 7 が実行するようにしてもよい。図 3 9 は、オブジェクトプログラムを暗号化する処理を説明するフローチャートである。ステップ S 5 4 1 において、パーソナルコンピュータ 1 は、ソースプログラムをコンパイルし、所定のオブジェクトプログラムを生成する。ステップ S 5 4 2 乃至ステップ S 5 4 6 の処理は、図 3 7 のステップ S 5 0 1 乃至ステップ S 5 0 5 とそれぞれ同様の処理なので、その説明は省略する。

【 0 1 3 5 】

図 4 0 は、暗号化されたオブジェクトプログラムをアダプタ 7 が実行する処理を説明するフローチャートである。ステップ S 5 6 1 において、アダプタ 7 の CPU 3 2 は、パーソナルコンピュータ 1 から受信した、暗号化されたオブジェクトプログラムを、不揮発性メモリ 3 4 に予め記憶されている認証局の公開鍵で復号する。ステップ S 5 6 2 において、アダプタ 7 の CPU 3 2 は、復号されたオブジェクトプログラムを RAM 3 3 に展開し、実行する。ステップ S 5 6 3 乃至ステップ S 5 6 5 は、図 3 8 のステップ 5 2 3 乃至ステップ S 5 2 5 とそれぞれ同様の処理なので、その説明は省略する。

【 0 1 3 6 】

次に、オブジェクトプログラムを暗号化する他の処理を、図 4 1 のフローチャートを参照して説明する。ステップ S 5 8 1 において、パーソナルコンピュータ 1 の CPU 1 2 は、ソースプログラムをコンパイルし、オブジェクトプログラム

を生成する。ステップS582において、パーソナルコンピュータ1のCPU12は、インターフェース17を介して、アダプタ7にアプリケーション鍵K_{ap}および個別鍵K_{idv}の発行を要求する。

【0137】

ステップS583において、パーソナルコンピュータ1は、インターフェース17を介して、アダプタ7からアプリケーション鍵K_{ap}および個別鍵K_{idv}（アダプタ7の不揮発性メモリ34に記憶されている、アダプタ7固有の鍵K_sを基に、生成される）を受信する。ステップS584において、パーソナルコンピュータ1のCPU12は、オブジェクトプログラムをアプリケーション鍵K_{ap}で暗号化する。ステップS585において、パーソナルコンピュータ1のCPU12は、コンテキストに含まれるマスター鍵KM_bなどを個別鍵K_{idv}で暗号化する。ステップS586において、パーソナルコンピュータ1のCPU12は、アプリケーション鍵K_{ap}で暗号化されたオブジェクトプログラム、および個別鍵K_{idv}で暗号化されたコンテキストに含まれるマスター鍵KM_bなどをハードディスク15に記録させ、処理は終了する。

【0138】

このように、パーソナルコンピュータ1は、アダプタ7から供給されたアプリケーション鍵K_{ap}および個別鍵K_{idv}で、オブジェクトプログラムおよびコンテキストを暗号化することができる。

【0139】

図41のフローチャートに示される手順で暗号化されたオブジェクトプログラムをアダプタ7が実行する処理を、図42のフローチャートを参照して説明する。ステップS601において、パーソナルコンピュータ1のCPU12は、インターフェース17を介して、アダプタ7に、アプリケーション鍵K_{ap}で暗号化されたオブジェクトプログラム、および個別鍵K_{idv}で暗号化されたコンテキストに含まれるマスター鍵KM_bなどを送信する。

【0140】

ステップS602において、アダプタ7のCPU32は、不揮発性メモリ34に予め記憶されている鍵K_sおよびアプリケーション鍵K_{ap}に、ハッシュ関数

を適用し、個別鍵 K_{idv} を生成する。ステップ S603 において、アダプタ 7 の CPU 32 は、受信したオブジェクトプログラムをアプリケーション鍵 K_{ap} で復号する。ステップ S604 において、アダプタ 7 の CPU 32 は、コンテキストに含まれるマスター鍵 K_{Mb} などを個別鍵 K_{idv} で復号する。

【0141】

ステップ S605 において、アダプタ 7 の CPU 32 は、復号されたマスター鍵 K_{Mb} などを含むコンテキストを利用して、オブジェクトプログラムを実行する。ステップ S606 乃至ステップ S608 の処理は、図 38 のステップ S523 乃至ステップ S525 とそれぞれ同様なので、その説明は省略する。

【0142】

以上のように、図 42 のフローチャートで示される処理において、図 41 のフローチャートで個別鍵 K_{idv} を送信したアダプタ 7 は、暗号化されたオブジェクトプログラムを実行することができる。従って、図 41 のフローチャートで個別鍵 K_{idv} を送信したアダプタ 7 以外のアダプタは、オブジェクトプログラムを復号できるが、コンテキストを復号できず、暗号化されたオブジェクトプログラムは実行できない。

【0143】

次に、アダプタ 7 がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ 1 の CPU 12 に実行させるときの処理を図 43 のフローチャートを参照して説明する。ステップ S651 において、アダプタ 7 の CPU 32 は、オブジェクトプログラムの所定の命令列を、所定の規則に従って、変換する。

【0144】

この変換は、例えば、DES の暗号化または復号のプログラムの場合、Feistel 構造などの基本構造を繰り返す処理のとき、いわゆる F 関数で利用される 48 ビットの拡大鍵と適切な乱数とに排他的論理和を所定の回数、適用するなどの変換を実行し、拡大鍵を解読しにくくする。また、例えば、DES CBC (Cipher Block Chaining) Mode で、多量のデータを復号するプログラムの場合、繰り返し構造の処理を順 (シーケンシャル) に実行せず、多量のデータに対し、

複数の繰り返し構造の処理を同時に実行し、拡大鍵を解読しにくくする。

【0145】

また、例えば、ソースプログラムのインストラクションに対応するコード（例えば、加算を表すコードが”1”に対応し、乗算を表すコードが”2”に対応する）を毎回変更する。

【0146】

ステップS652において、アダプタ7のCPU32は、変換された命令列を、インターフェース31を介して、パーソナルコンピュータ1に送信する。

【0147】

ステップS653において、パーソナルコンピュータ1のCPU12は、デシヤッフルされた命令列を実行する。ステップS654において、パーソナルコンピュータ1のCPU12は、命令列を実行して得られた処理結果をアダプタ7に送信する。

【0148】

ステップS655において、アダプタ7のCPU32は、パーソナルコンピュータ1から受信した処理結果、およびアダプタ7のCPU32が算出し保持している計算結果を基に、処理を継続する。ステップS656において、アダプタ7のCPU32は、パーソナルコンピュータ1に処理を実行させるか否かを判定し、パーソナルコンピュータ1に処理を実行させないと判定された場合、処理は終了する。ステップS656において、パーソナルコンピュータ1に処理を実行させると判定された場合、手続きは、ステップS651に戻り、パーソナルコンピュータ1に処理を実行させる処理を繰り返す。

【0149】

以上のように、アダプタ7は、オブジェクトプログラムの処理の一部をパーソナルコンピュータ1に実行させることにより、高速にかつ安全に、オブジェクトプログラムの処理を実行することができる。

【0150】

アダプタ7は、オブジェクトプログラムに含まれる命令列を変換してパーソナルコンピュータ1に送信することにより、オブジェクトプログラムの解読が困難

になる。アダプタ 7 が、オブジェクトプログラムに含まれる命令列を暗号化して、パーソナルコンピュータ 1 に送信すれば、オブジェクトプログラムの解読は更に困難になる。

【0151】

なお、図 4 1 で説明したパーソナルコンピュータ 1 がアダプタ 7 に供給するオブジェクトプログラムを暗号化する処理において、ソースプログラムに対しステップ S 6 5 1 に示した変換を実行すれば、オブジェクトプログラムの解読は更に困難になる。

【0152】

最後に、パーソナルコンピュータ 1 が EMD サーバ 5 から、事前に無料でダウンロードした音楽データを暗号化している暗号鍵をダウンロードするとともに、決済をする処理を、図 4 4 のフローチャートを参照して説明する。ステップ S 6 7 1 において、パーソナルコンピュータ 1 は、インターネット 4 を介して、EMD サーバ 5 と相互認証する。ステップ S 6 7 2 において、パーソナルコンピュータ 1 の CPU 1 2 は、インターネット接続インターフェース 1 1 を介して、EMD サーバ 5 に、音楽データの再生条件を示すデータを送信する。ステップ S 6 7 3 において、EMD サーバ 5 は、受信した再生条件を示すデータを基に、支払い金額のデータをパーソナルコンピュータ 1 に送信する。

【0153】

ステップ S 6 7 4 において、パーソナルコンピュータ 1 の CPU 1 2 は、EMD サーバ 5 から受信した支払い金額のデータをディスプレイ 3 に表示させる。ステップ S 6 7 5 において、EMD サーバ 5 は、パーソナルコンピュータ 1 に、ユーザのクレジットカードの番号等の送信を要求する。ステップ S 6 7 6 において、ユーザは、入力部 2 を操作し、パーソナルコンピュータ 1 にクレジットカードの番号等のデータを入力し、パーソナルコンピュータ 1 は、クレジットカードの番号等のデータを EMD サーバ 5 に送信する。

【0154】

ステップ S 6 7 7 において、EMD サーバ 5 は、パーソナルコンピュータ 1 から受信したクレジットカードの番号等のデータを基に、決済の処理を実行する。

ステップ S 6 7 8 において、EMDサーバ 5 は、インターネット 4 を介して、パーソナルコンピュータ 1 に所定の暗号鍵を送信する。ステップ S 6 7 9 において、パーソナルコンピュータ 1 は、インターネット 4 を介して、EMDサーバ 5 から送信された所定の暗号鍵を受信し、処理は終了する。

【0155】

以上のように、パーソナルコンピュータ 1 が EMDサーバ 5 から暗号鍵をダウンロードするとともに、EMDサーバ 5 は、決済の処理をすれば、パーソナルコンピュータ 1 が EMDサーバ 5 から音楽データをダウンロードするとき、認証、暗号化、または決済などの処理が必要なくなるので、比較的大きなデータである音楽データを迅速にダウンロードすることができる。

【0156】

以上においては、記録媒体として、メモリスティックウォークマン 6 を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。クレジットカードの番号等のデータを基に、決済の処理を実行するとして説明したが、s m a s h (商標) などの手続きにより、決済をするようにしてもよい。

【0157】

また、図 4 4 のフローチャートに示す処理の前に、パーソナルコンピュータ 1 と EMDサーバ 5 とが、例えば、IS09798-3 で規定されている http (Hypertext Transport Protocol) 上のプロトコルを使用して、相互認証するようにしてもよい。

【0158】

なお、メモリスティックウォークマン 6 は、予め個別鍵を記憶しているとして説明したが、ユーザがメモリスティックウォークマン 6 を購入後、EMDサーバ 5 などからダウンロードするようにしてもよい。

【0159】

また、データは、音楽データ以外に、画像データ、その他のデータとすることもできる。

【0160】

以上のように、本発明によれば、次のような効果を奏することができる。

【0161】

(1) ハードディスク15に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上でハードディスク15に記録するようにしたので、ハードディスク15に記録されている音楽データをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

【0162】

(2) 所定の曲を1回コピーしたとき、一定時間(上記例の場合、48時間)の間、その曲をコピーすることができないようするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

【0163】

さらにデータベースを更新する度に、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

【0164】

(3) 外部の装置に音楽データを渡したら、ハードディスク15上の音楽データを消去するようにしたので、ハードディスク15内に元のデジタル音楽データが残らず、その複製を大量に配布することが防止される。

【0165】

(4) ハードディスク15内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、ハードディスク15の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをハードディスク15にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

【0166】

(5) パーソナルコンピュータ1が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

【0167】

(6) 外部機器から、パーソナルコンピュータ 1 に対してデータを渡す前に、パーソナルコンピュータ 1 のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対して音楽データを渡してしまうようなことが防止される。

【0168】

(7) 曲の同一性の判定に ISRC を用い、ISRC が取得できないときは、TOC を用いるようにしたので、ISRC が取得できなくとも、曲の同一性を判定することが可能になる。

【0169】

(8) パーソナルコンピュータ 1 におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ 1 に外付けされるアダプタ 7 に負担させるようにしたので、パーソナルコンピュータ 1 のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

【0170】

更に、そのソフトウェアが、安全な認証局または EMD サーバ 5 で暗号化またはシャッフルされるので、ソフトウェアの改竄は、より困難となる。

【0171】

(9) プログラムをプログラムに対応する鍵で暗号化し、プログラムの実行に必要なデータを、アダプタ 7 が生成する固有の鍵で暗号化するようにしたので、プログラムのみを CD-ROM などの媒体で配布可能にしつつ、プログラムを他のアダプタ 7 で実行することが防止される。

【0172】

(10) 音楽データなどのコンテンツを暗号化する鍵をダウンロードするとき、決済されるようにしたので、比較的大きなデータである音楽データなどのコンテンツを迅速にダウンロードすることができるようになる。

【0173】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0 1 7 4】

なお、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0 1 7 5】

【発明の効果】

請求項 1 に記載の情報処理装置、請求項 4 に記載の情報処理方法、および請求項 5 に記載の提供媒体によれば、半導体 I C に実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体 I C に送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

【0 1 7 6】

請求項 6 に記載の情報処理システムによれば、半導体 I C に実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体 I C に送信され、半導体 I C に実行させるプログラムが受信されるとともに、情報処理装置に暗号化されたプログラムが送信され、受信したプログラムが所定の方式で暗号化されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

【図面の簡単な説明】

【図 1】

本発明を適用したシステムの構成例を示すブロック図である。

【図 2】

図 1 のシステムにおいてコンパクトディスクからハードディスク 1 5 にコピーする場合の処理を説明するフローチャートである。

【図 3】

図 2 のステップ S 1 2 の期限データベースチェック処理を説明するフローチャートである。

【図 4】

期限データベースの例を示す図である。

【図 5】

ウォータマークを説明する図である。

【図 6】

曲データベースの例を示す図である。

【図 7】

図 1 のシステムのハードディスク 15 からメモリスティックウォークマン 6 ヘデータを移動する動作を説明するフローチャートである。

【図 8】

図 1 のシステムのハードディスク 15 からメモリスティックウォークマン 6 ヘデータを移動する動作を説明するフローチャートである。

【図 9】

図 1 のシステムのハードディスク 15 からメモリスティックウォークマン 6 ヘデータを移動する作を説明するフローチャートである。

【図 10】

図 7 のステップ S 5 5 の選択曲の再生条件などのチェック処理を説明するフローチャートである。

【図 11】

メモリスティックウォークマンが管理している再生条件を説明する図である。

【図 12】

図 7 のステップ S 5 8 のフォーマット変換処理の詳細を説明するフローチャートである。

【図 13】

図 1 のハードディスク 15 からメモリスティックウォークマン 6 ヘデータをコピーする場合の動作を説明するフローチャートである。

【図 14】

図 1 のハードディスク 15 からメモリスティックウォークマン 6 ヘデータをコピーする場合の動作を説明するフローチャートである。

【図 15】

図 1 のハードディスク 15 からメモリスティックウォークマン 6 ヘデータをコピーする場合の動作を説明するフローチャートである。

【図 16】

図 1 のメモリスティックウォークマン 6 からハードディスク 15 ヘデータを移動する場合の動作を説明するフローチャートである。

【図 17】

図 1 のシステムのメモリスティックウォークマン 6 からハードディスク 15 ヘデータをコピーする場合の動作を説明フローチャートである。

【図 18】

図 1 のシステムの EMD サーバ 5 からハードディスク 15 ヘデータをコピーする場合の処理を説明するフローチャートである。

【図 19】

図 18 のステップ S 204 の課金に関する処理の詳細を説明するフローチャートである。

【図 20】

課金ログを説明する図である。

【図 21】

図 1 のシステムの IEC 60958 端子 16 a からハードディスク 15 ヘデータをコピーする 2 合の処理を説明するフローチャートである。

【図 22】

図 1 のシステムの IEC 60958 端子 16 a からハードディスク 15 ヘデータをコピーする場合の処理を説明するフローチャートである。

【図 23】

図 1 のシステムのハードディスク 15 から IEC 60958 端子 16 a にデータを出力する場合の動作を説明するフローチャートである。

【図 24】

図 1 のシステムのハードディスク 15 から IEC 60958 端子 16 a にデータを出力する場合の動作を説明するフローチャートである。

【図 25】

図 23 のステップ S 275 の再生条件などのチェック処理を説明するフローチャートである。

【図 26】

図 1 のシステムのハードディスク 15 からメモリスティックウォークマン 6 経由でデータを出力する場合の動作を説明するフローチャートである。

【図 27】

図 1 のシステムのハードディスク 15 からメモリスティックウォークマン 6 経由でデータを出力する場合の動作を説明するフローチャートである。

【図 28】

図 1 の不揮発性メモリ 34 の機能を説明する図である。

【図 29】

図 1 のシステムのアダプタ 7 の動作を説明するフローチャートである。

【図 30】

図 1 のシステムのアダプタ 7 の内部の構成を示す図である。

【図 31】

図 31 の不揮発性メモリ 34 の内部の構成例を示す図である。

【図 32】

図 31 の不揮発性メモリ 34 の内部の構成例を示す図である。

【図 33】

アダプタ 7 とパーソナルコンピュータ 1 との相互認証の処理を説明するフローチャートである。

【図 34】

アダプタ 7 とパーソナルコンピュータ 1 との相互認証の処理を説明するフローチャートである。

【図 35】

アダプタ 7 とパーソナルコンピュータ 1 との相互認証の処理を説明するフローチャートである。

【図 36】

アダプタ 7 とパーソナルコンピュータ 1 との相互認証の処理を説明するフローチャートである。

【図 3 7】

ソースプログラムを暗号化する処理を説明するフローチャートである。

【図 3 8】

暗号化されたソースプログラムをアダプタ 7 が実行する処理を説明するフローチャートである。

【図 3 9】

オブジェクトプログラムを暗号化する処理を説明するフローチャートである。

【図 4 0】

暗号化されたオブジェクトプログラムをアダプタ 7 が実行する処理を説明するフローチャートである。

【図 4 1】

オブジェクトプログラムを暗号化する他の処理を説明するフローチャートである。

【図 4 2】

暗号化されたオブジェクトプログラムをアダプタ 7 が実行する他の処理を説明するフローチャートである。

【図 4 3】

アダプタ 7 がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ 1 の CPU 1 2 に実行させるときの処理を説明するフローチャートである。

【図 4 4】

パーソナルコンピュータ 1 が EMD サーバ 5 から暗号鍵をダウンロードするとともに、決済をする処理を説明するフローチャートである。

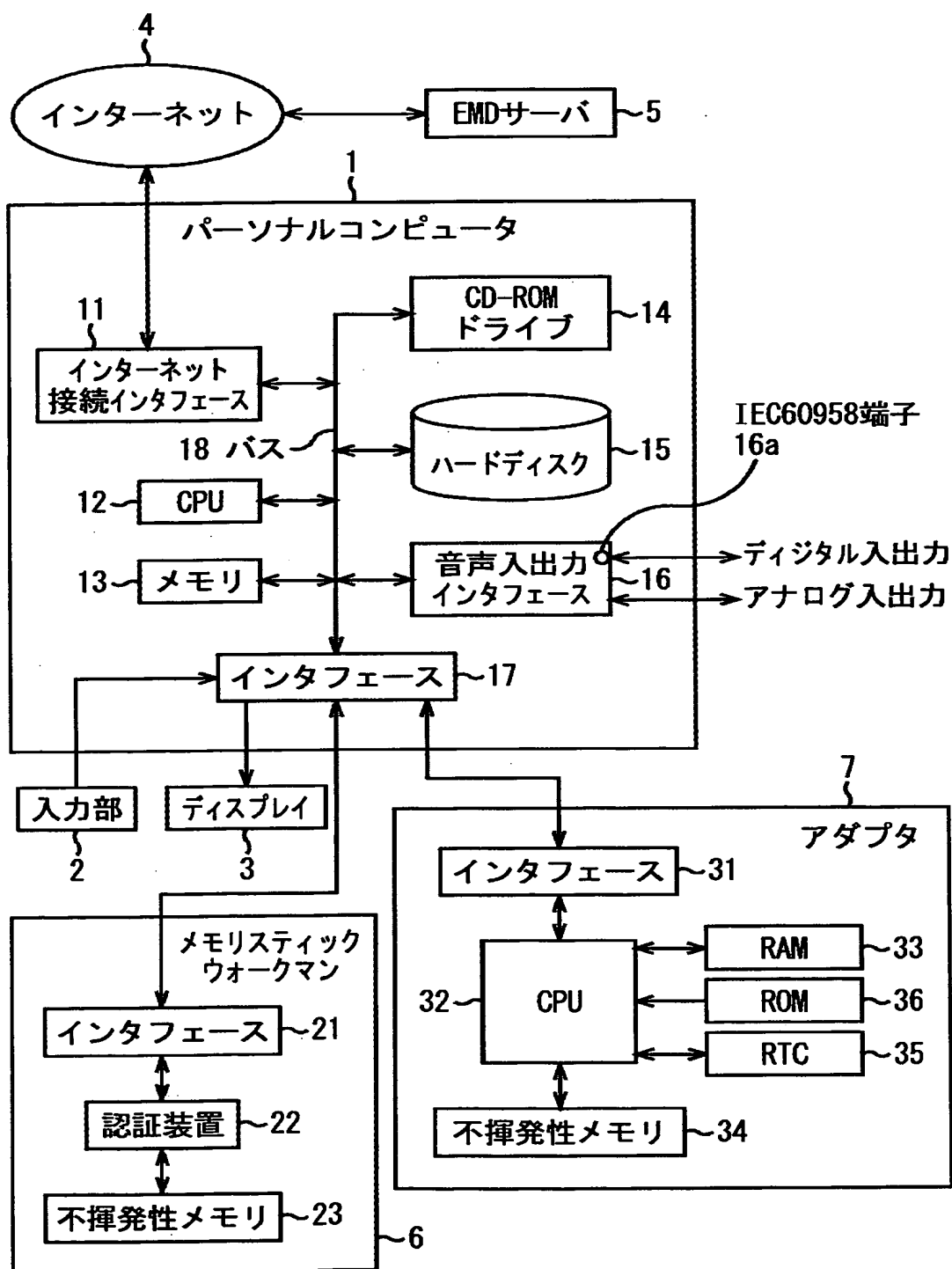
【符号の説明】

1 パーソナルコンピュータ, 2 入力部, 3 ディスプレイ, 4 インターネット, 5 EMDサーバ, 6 メモリスティックワークマン, 7 アダプタ, 12 CPU, 13 メモリ, 14 CD-ROMドライブ, 15

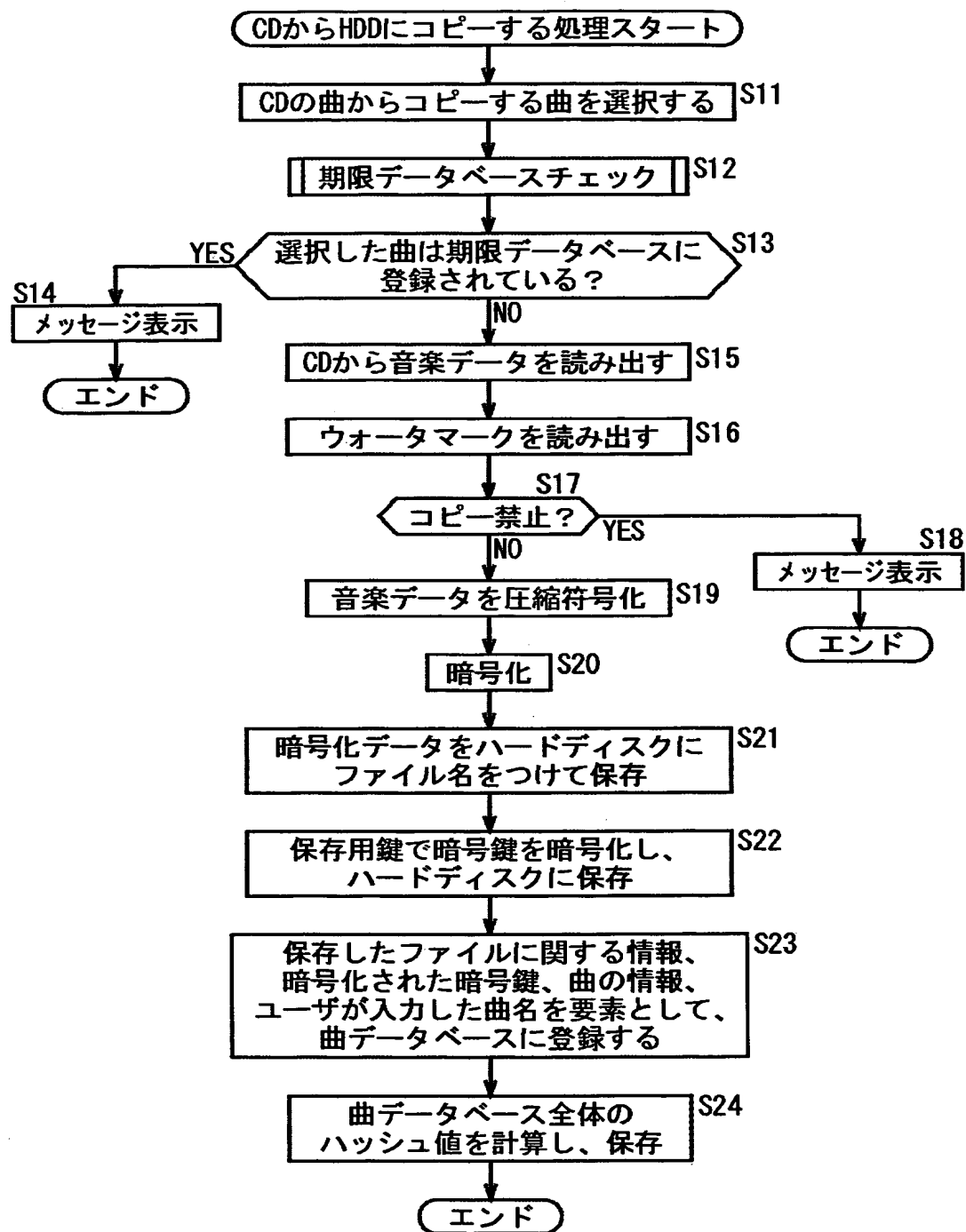
ハードディスク, 16 音声入出力インタフェース, 16 a IEC609
58 端子, 22 認証装置, 23 不揮発性メモリ, 32 CPU

【書類名】 図面

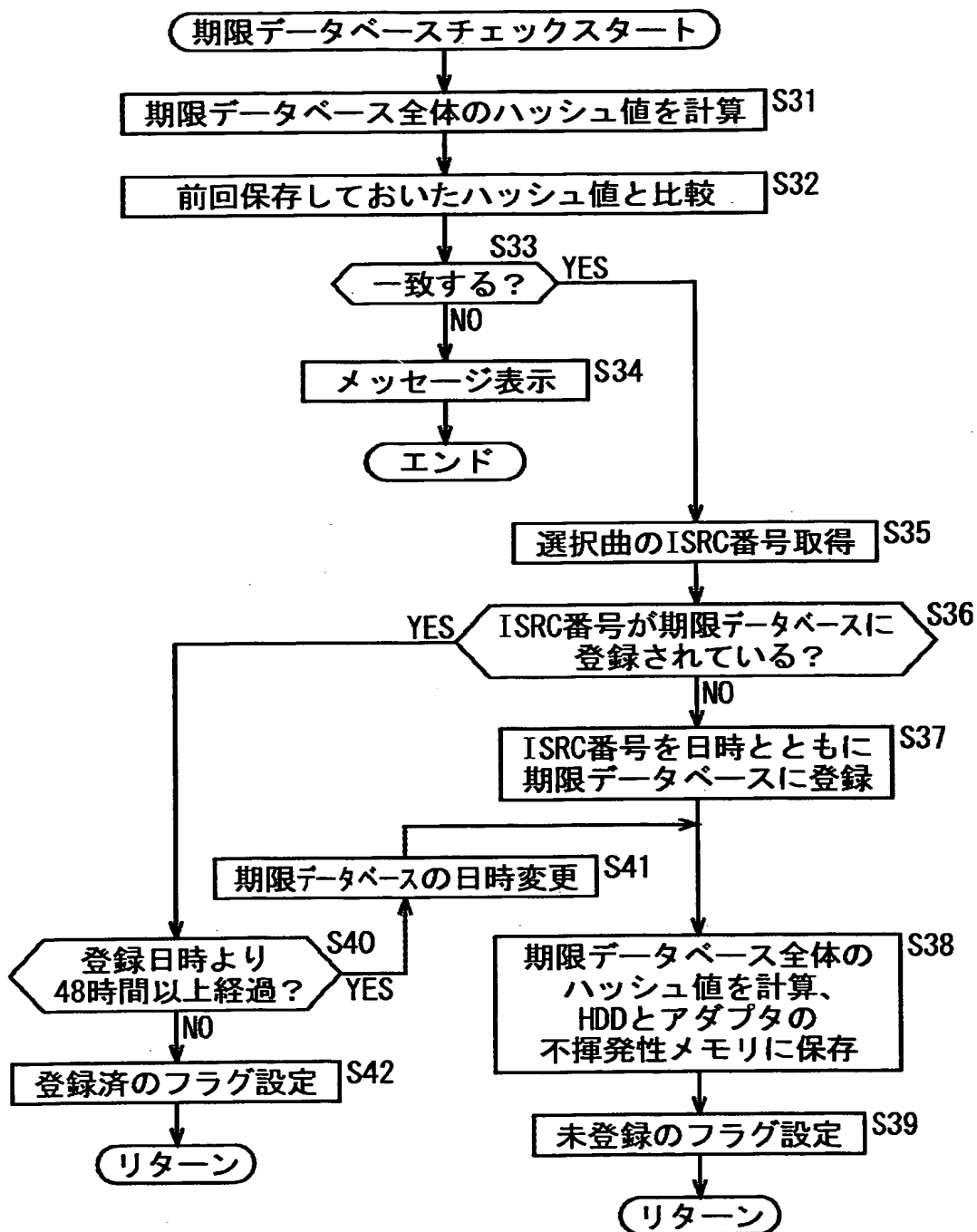
【図 1】



【図 2】



【図 3】



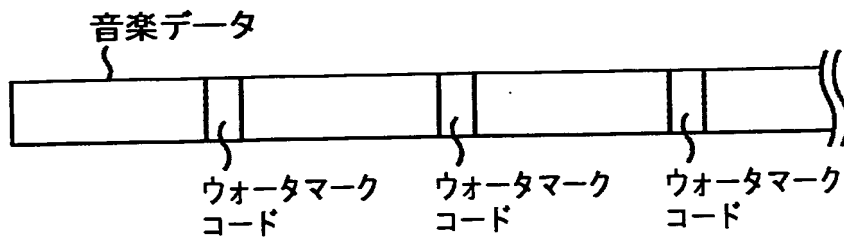
【図 4】

期限データベース

	アイテム1	アイテム2	アイテム3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

ハッシュ値	0xf3352e125934
-------	----------------

【図 5】



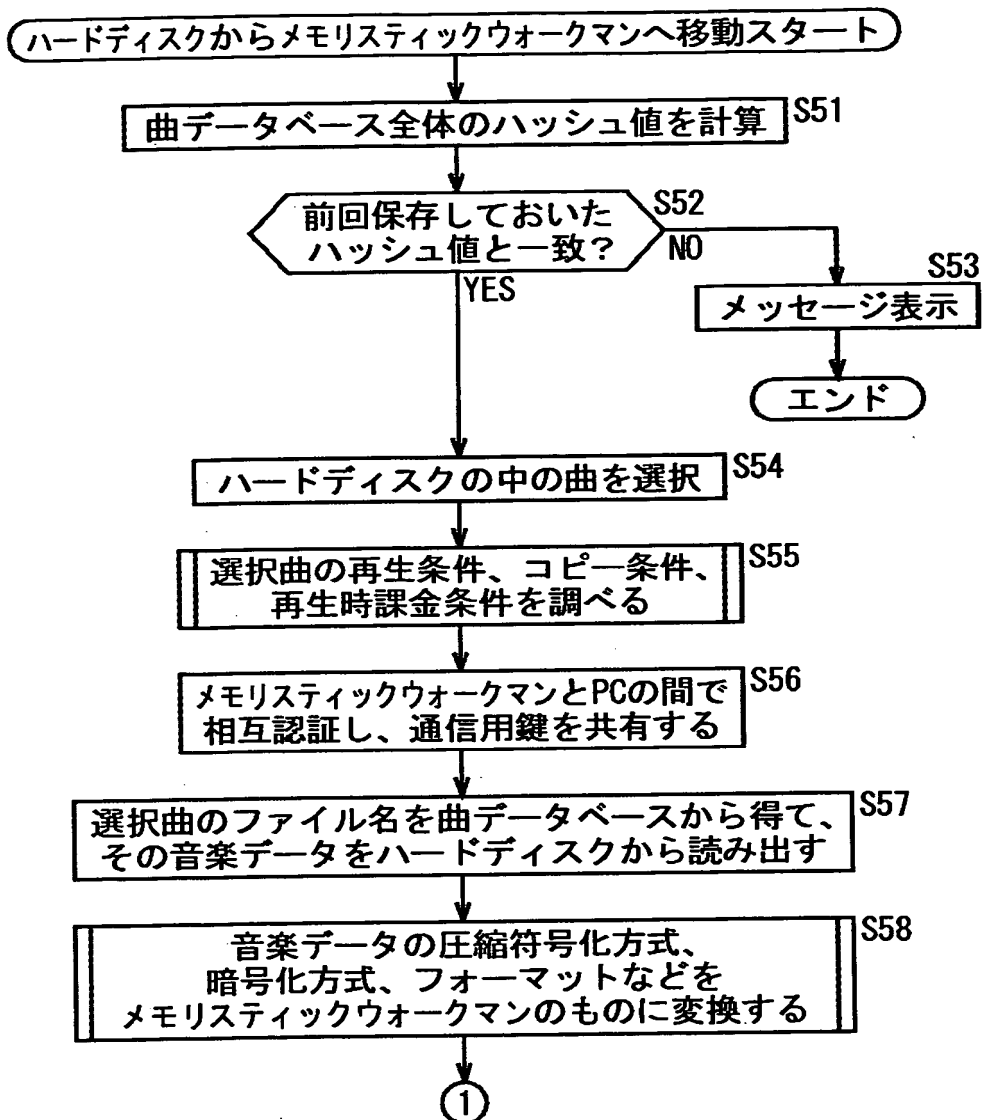
【図 6】

曲データベース

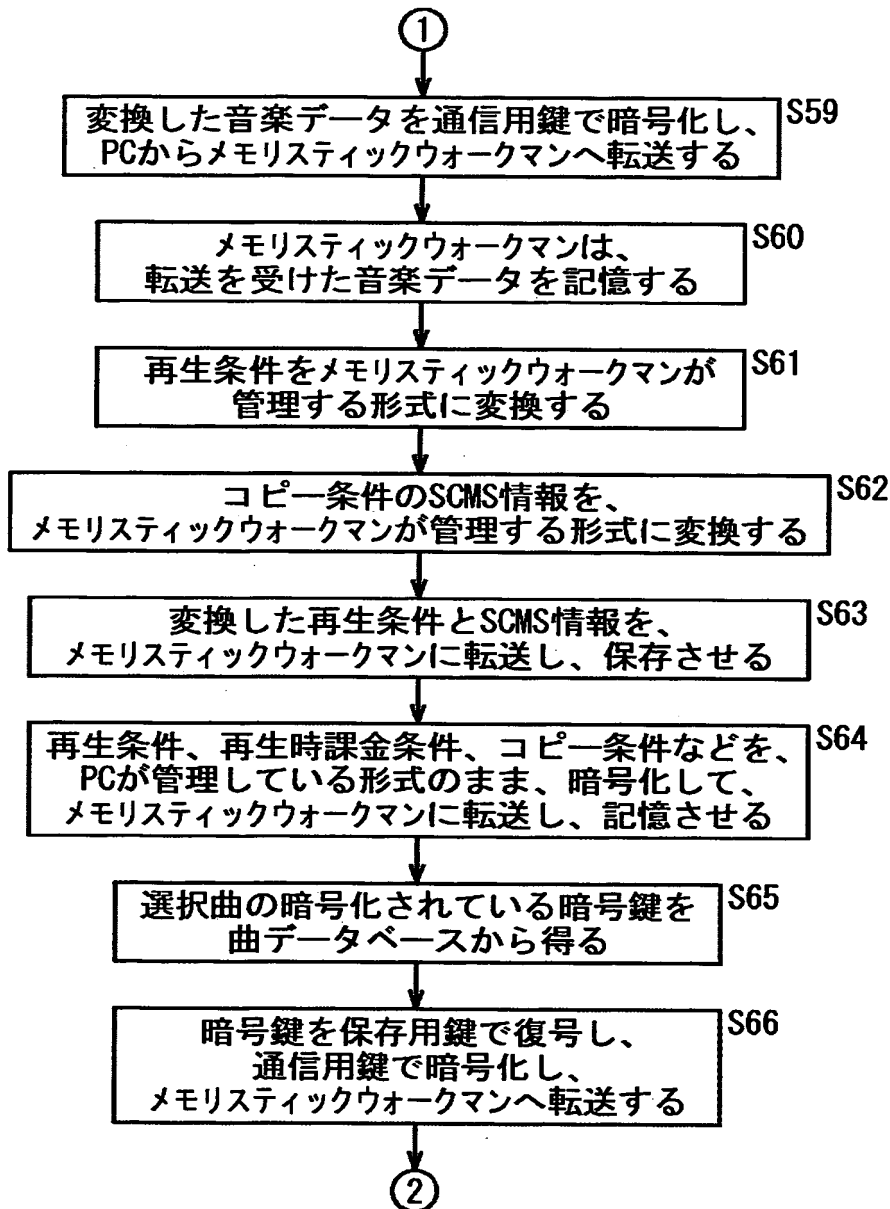
	アイテム1	アイテム2	アイテム3	
ファイル名	xd000110.at2	px92341234.at2	aa0234287034.at2	
暗号化された暗号鍵	0xabababababab	0x989898989898989	0x123456789012	
曲名	春の小川	運命	荒城の月	
長さ	180	190	200	
再生条件:開始日時	-	2001.01.01.00:00	-	
再生条件:終了日時	1999.07.31.23:59	-	-	
再生条件:回数制限	-	20	-	
再生回数カウンタ	-	12	-	
再生時課金条件	-	-	¥5	
コピー条件:回数	2	0	0	
コピー回数カウンタ	1	0	0	
コピー条件:SCMS	0b01	0b10	0b00	

ハッシュ値	0xf9951e566321
-------	----------------

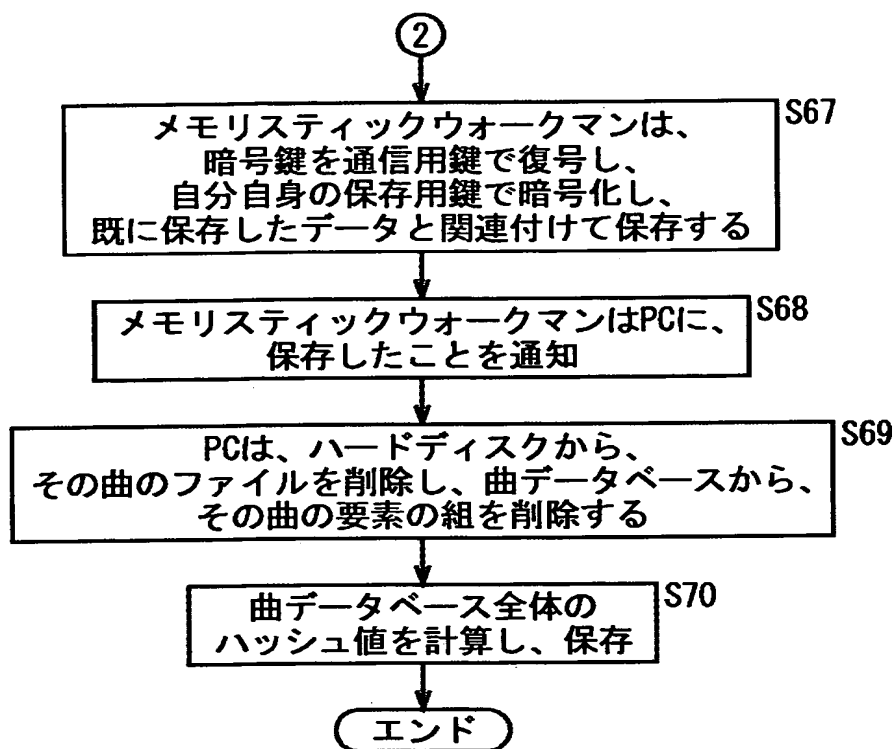
【図 7】



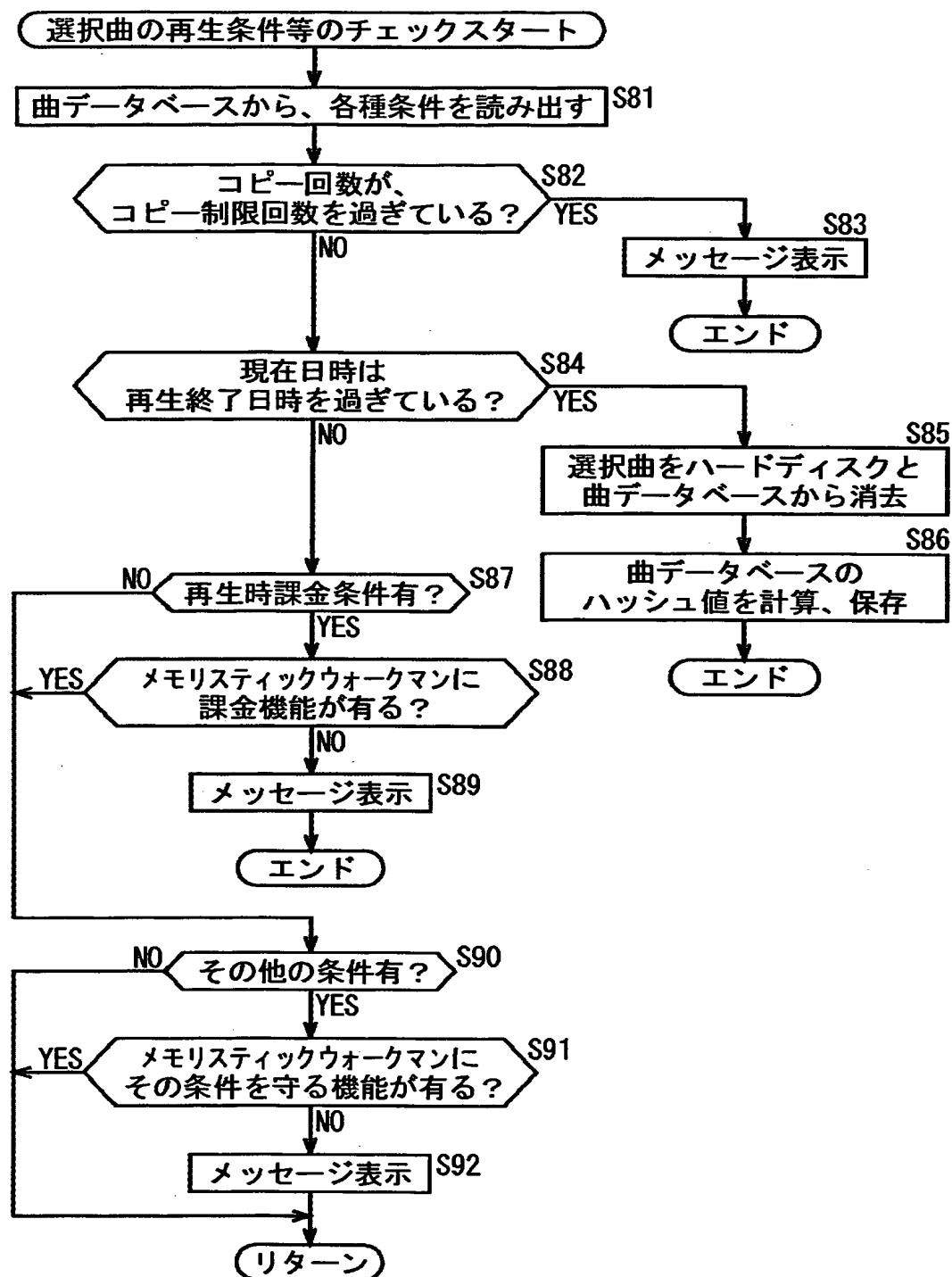
【図 8】



【図 9】



【図 10】

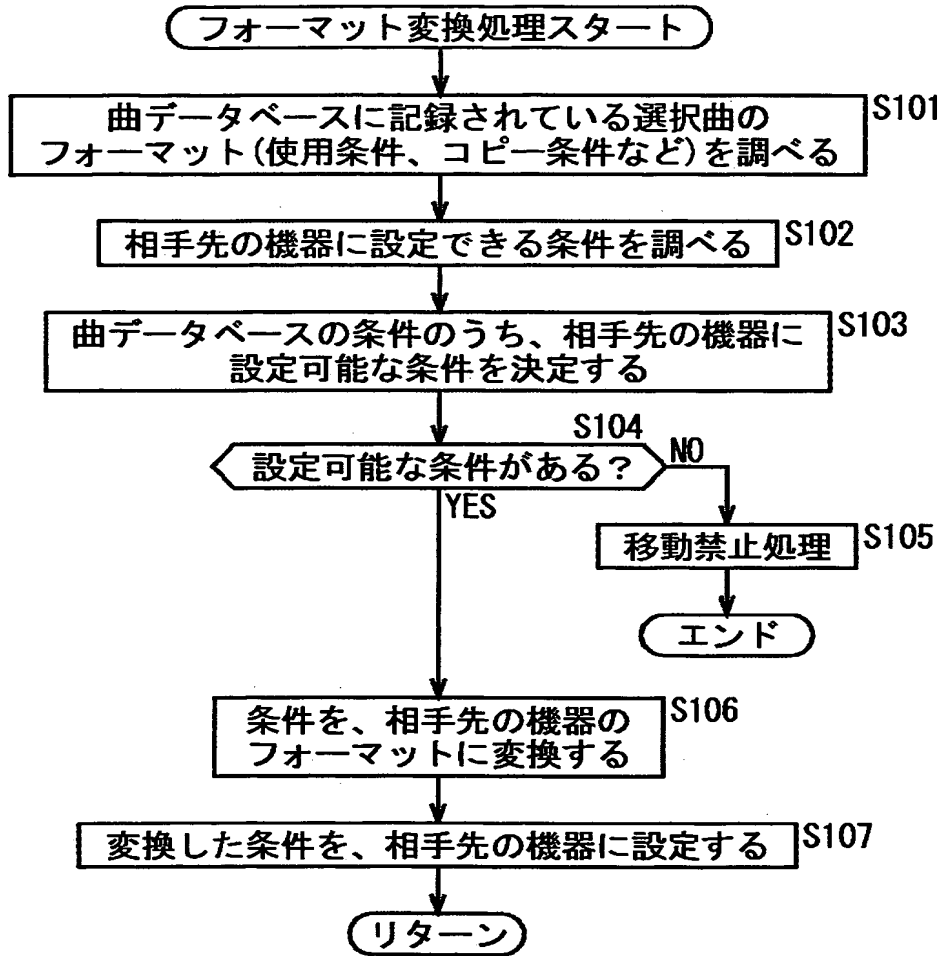


【図 1 1】

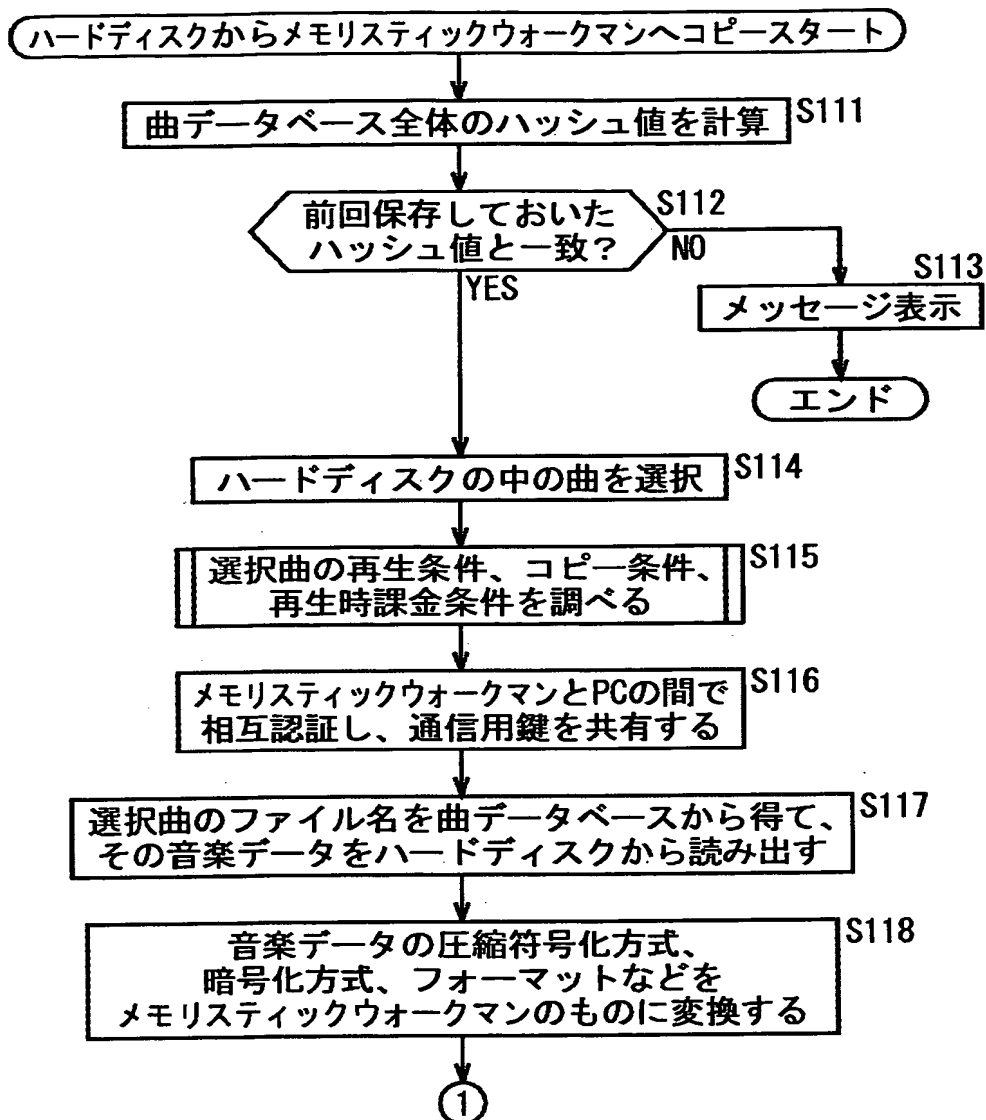
メモリスティックウォークマンが管理している再生条件

	アイテム1	アイテム2	アイテム3
曲ID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

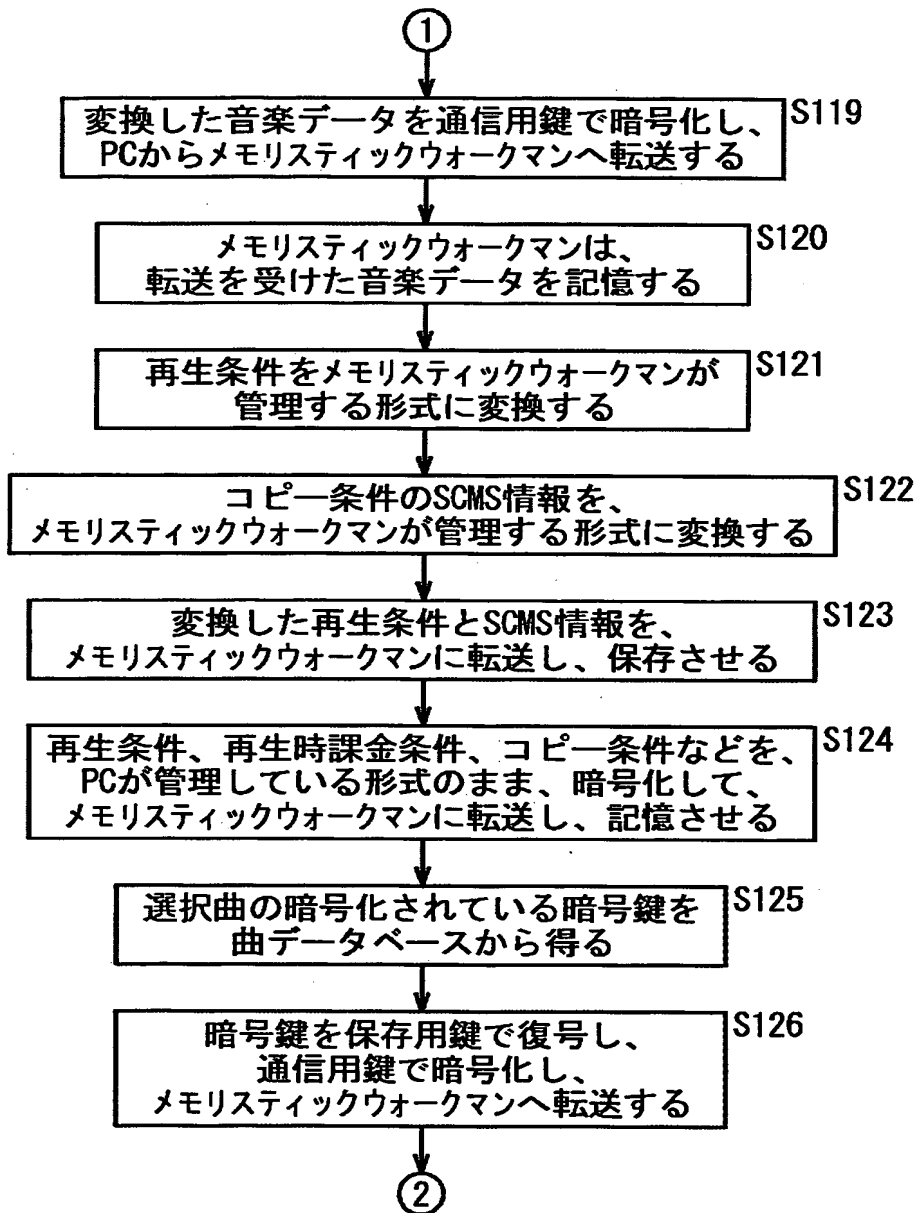
【図 1 2】



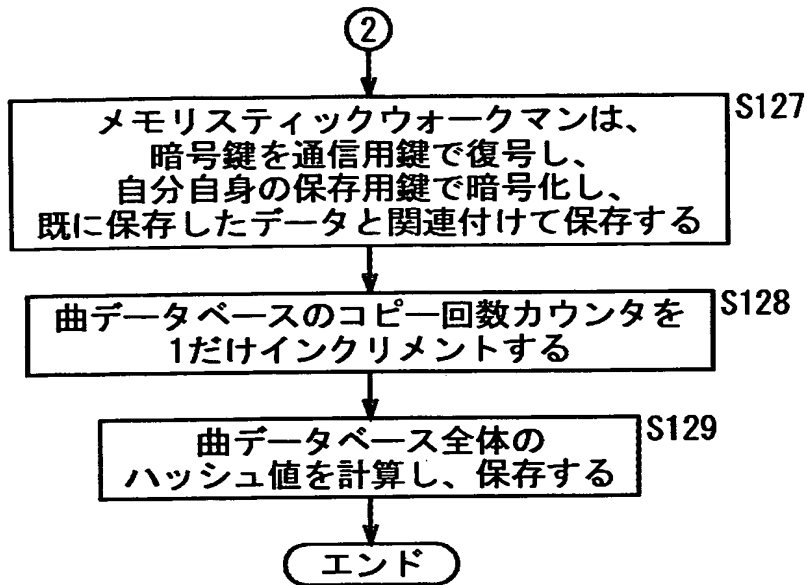
【図 13】



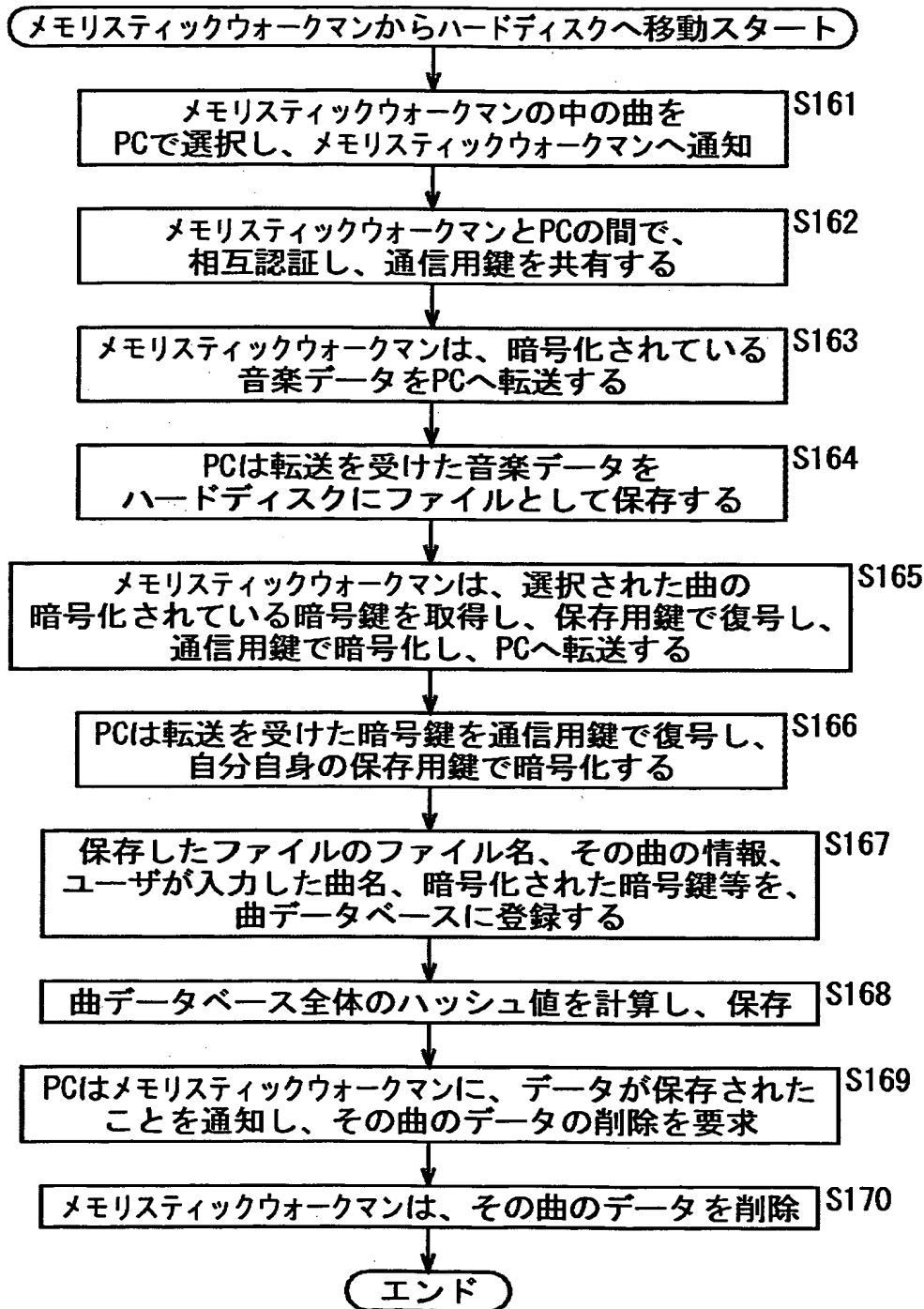
【図 14】



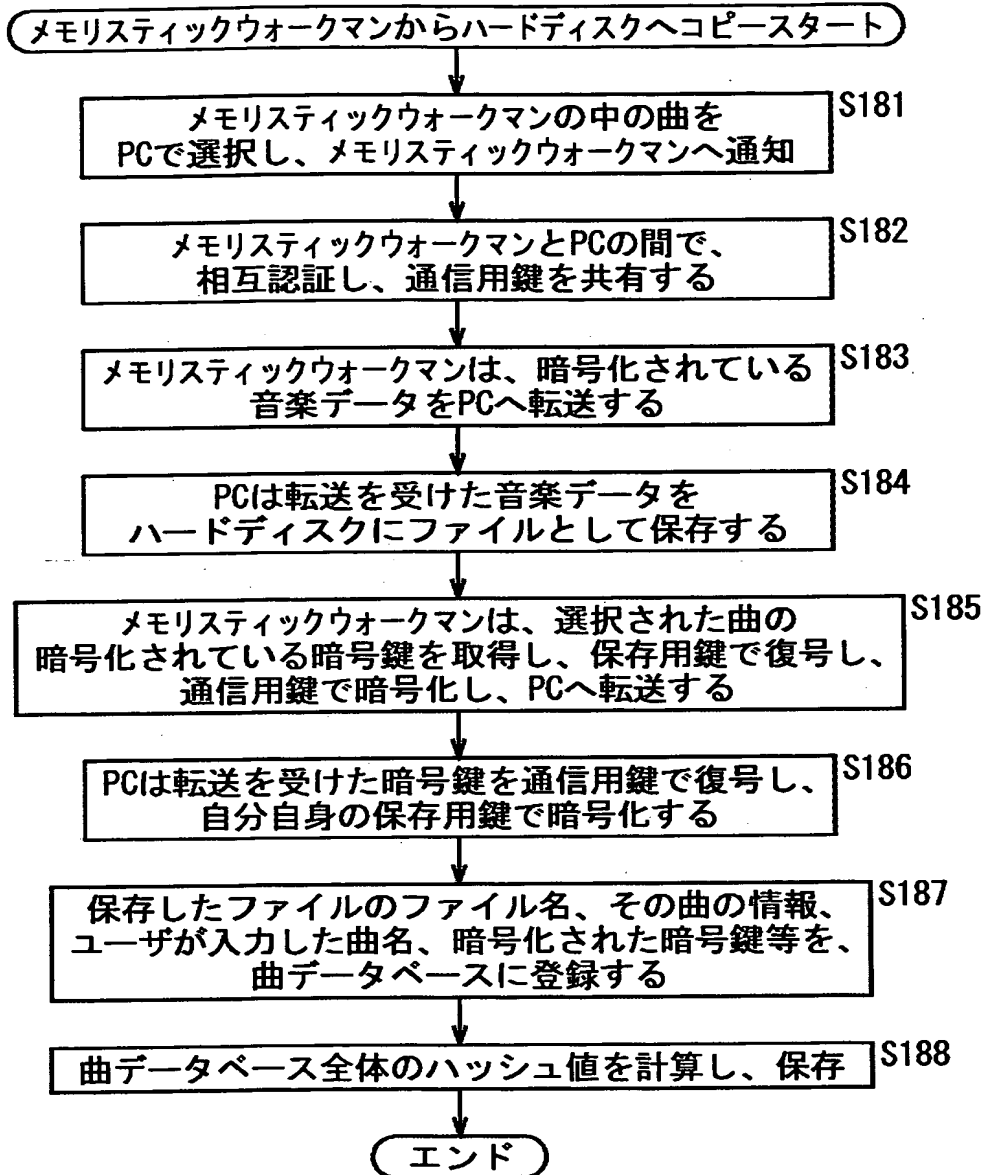
【図 15】



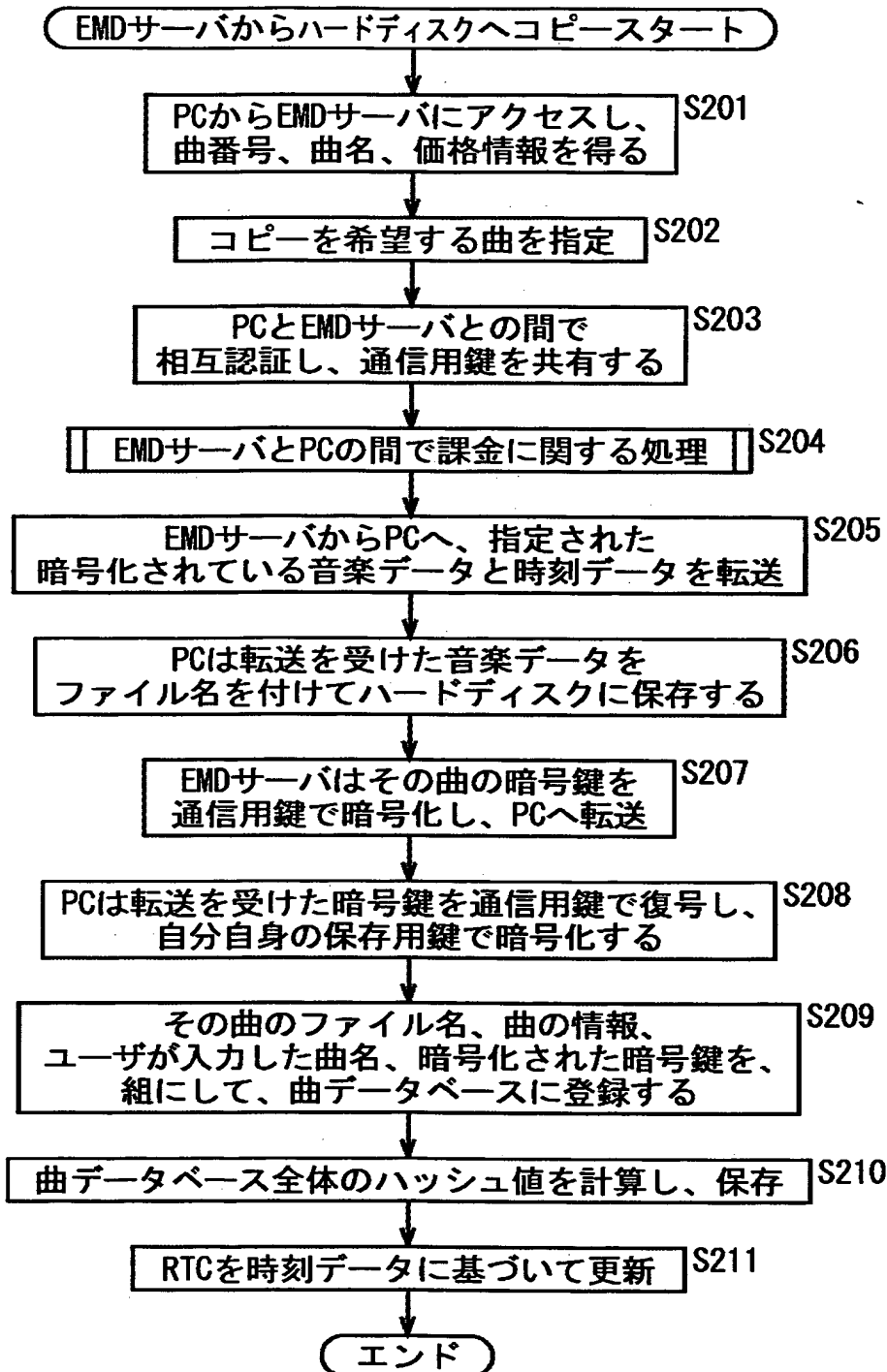
【図 16】



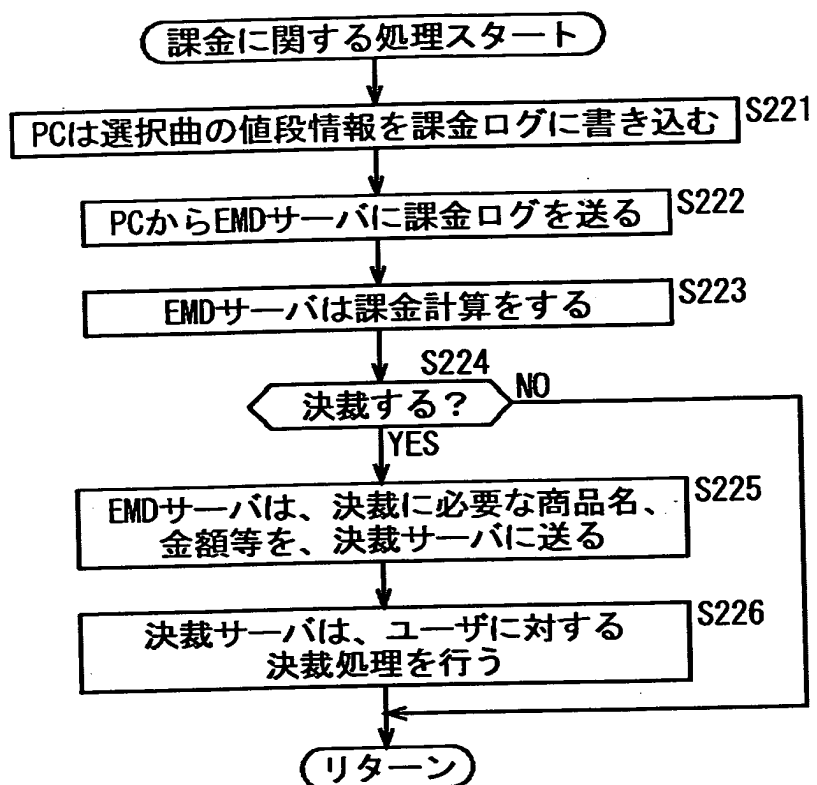
【図 17】



【図 1 8】



【図 1 9】



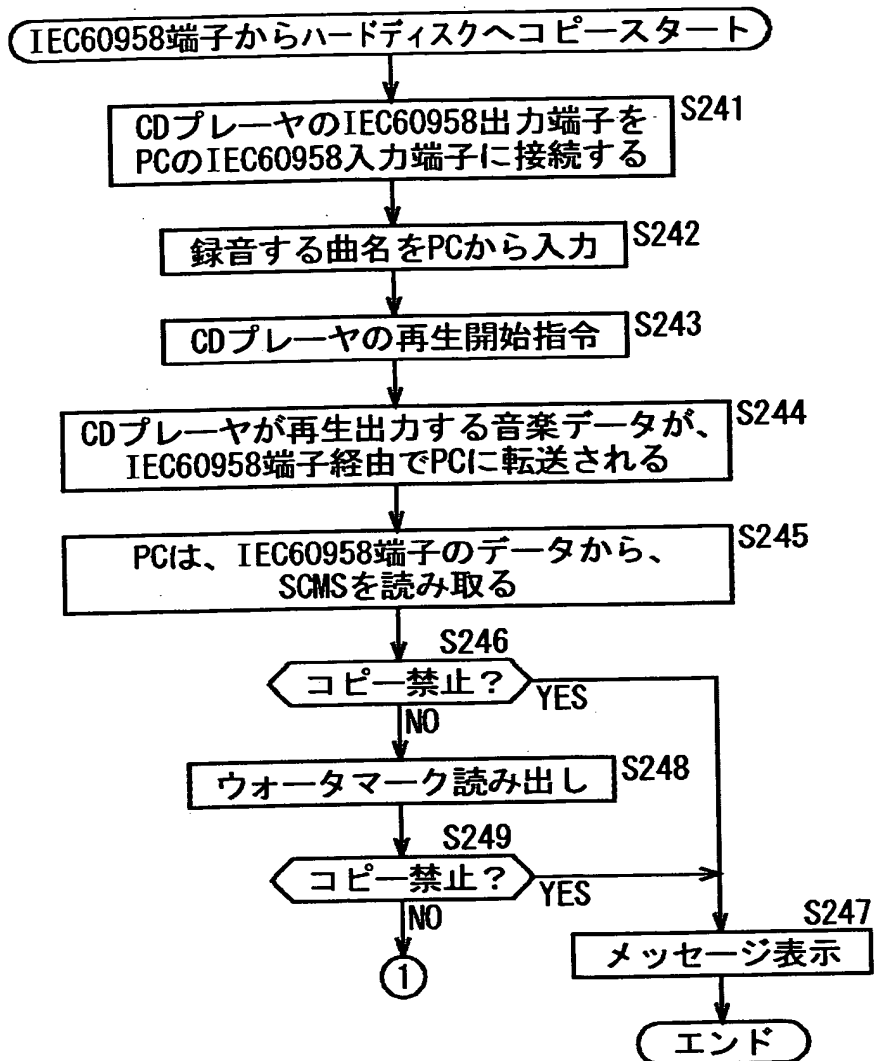
【図 20】

課金ログ

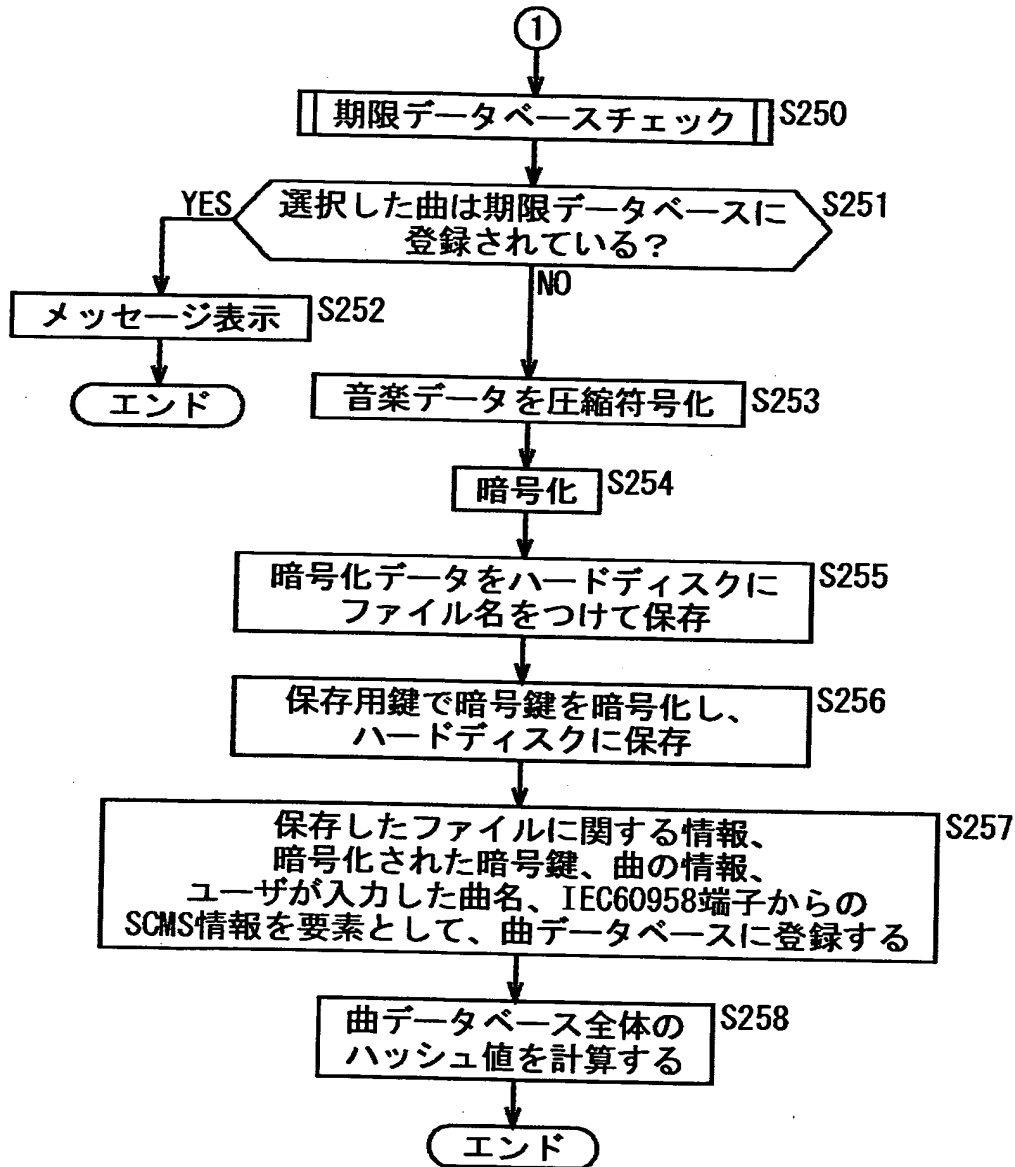
	アイテム1	アイテム2	アイテム3	
料金	50	50	60	

ハッシュ値	0xf8783e263517
-------	----------------

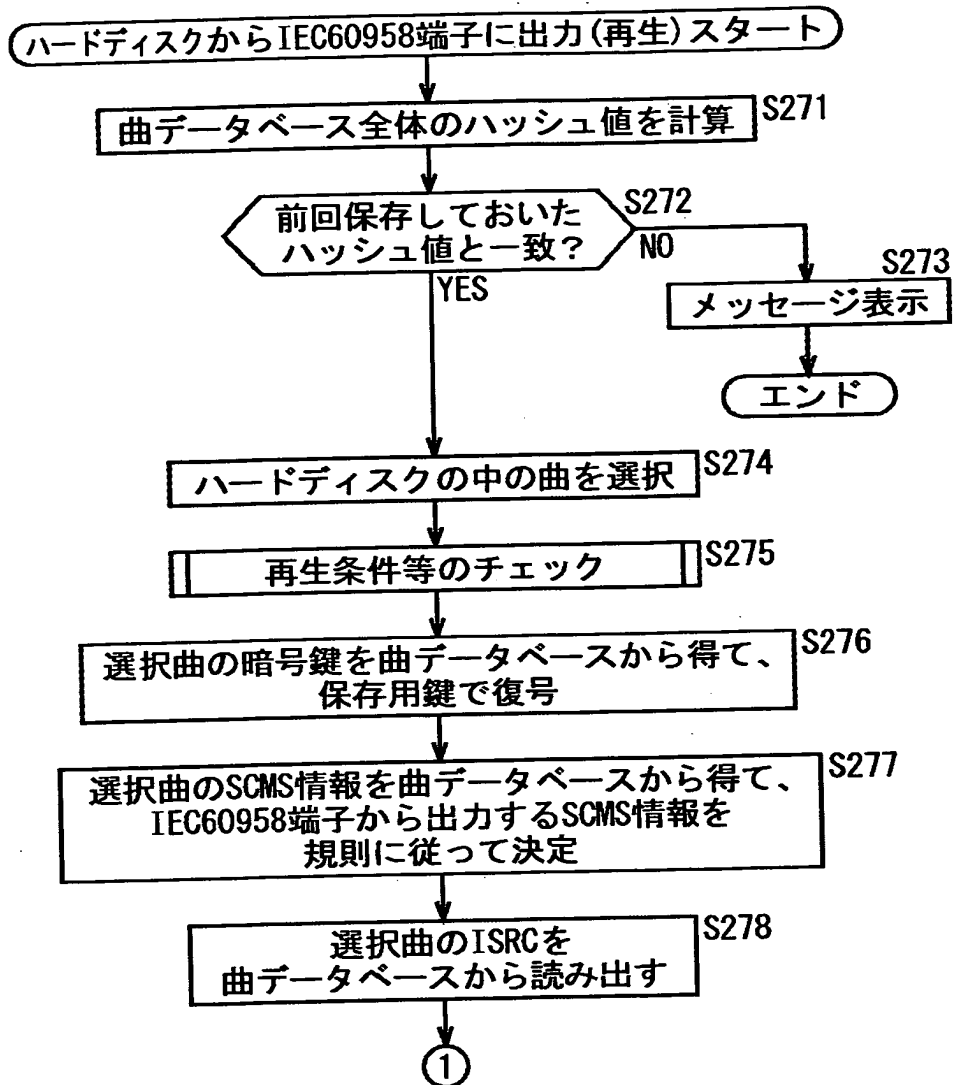
【図 21】



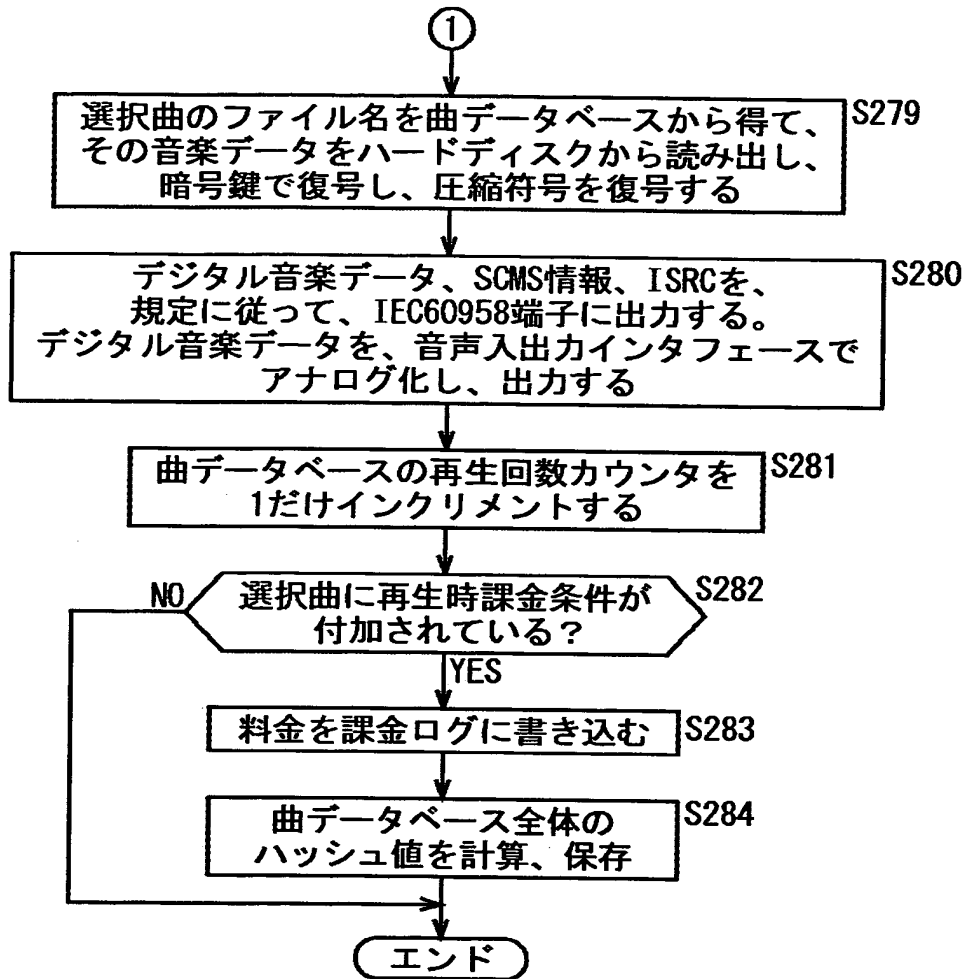
【図 22】



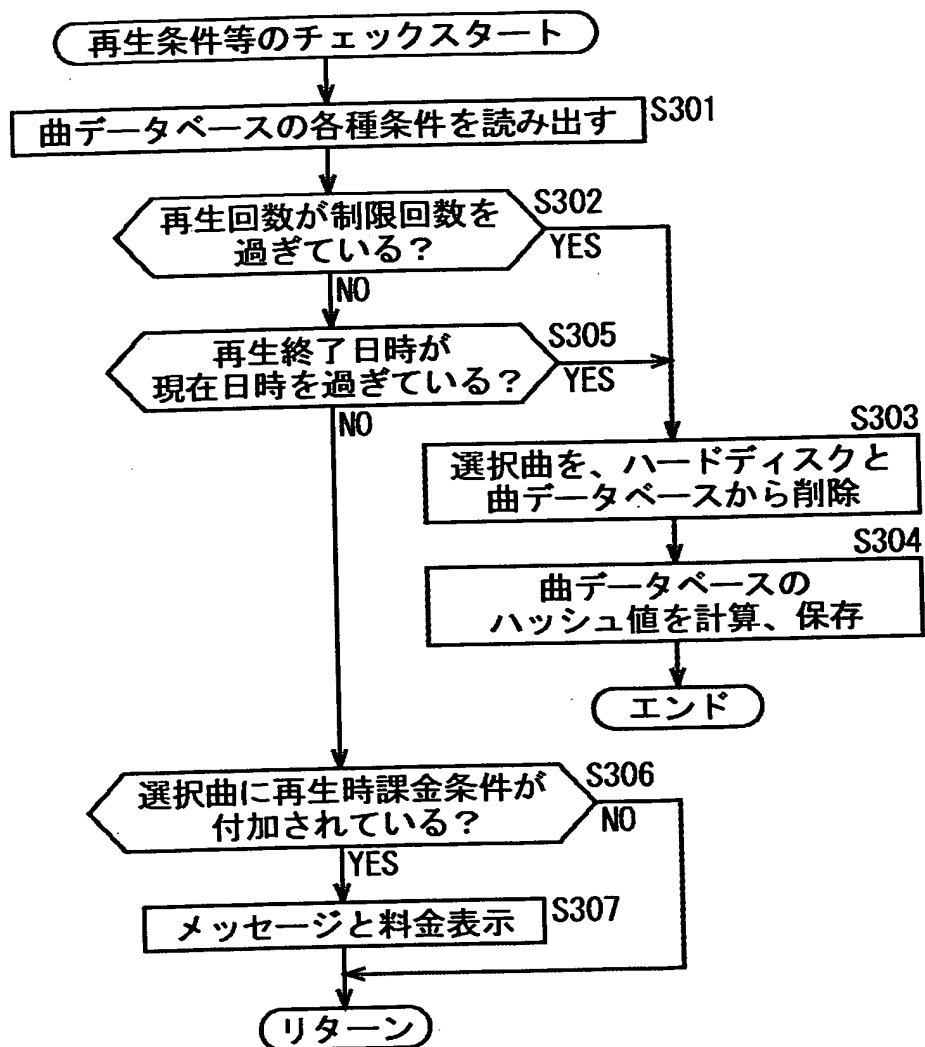
【図 2 3】



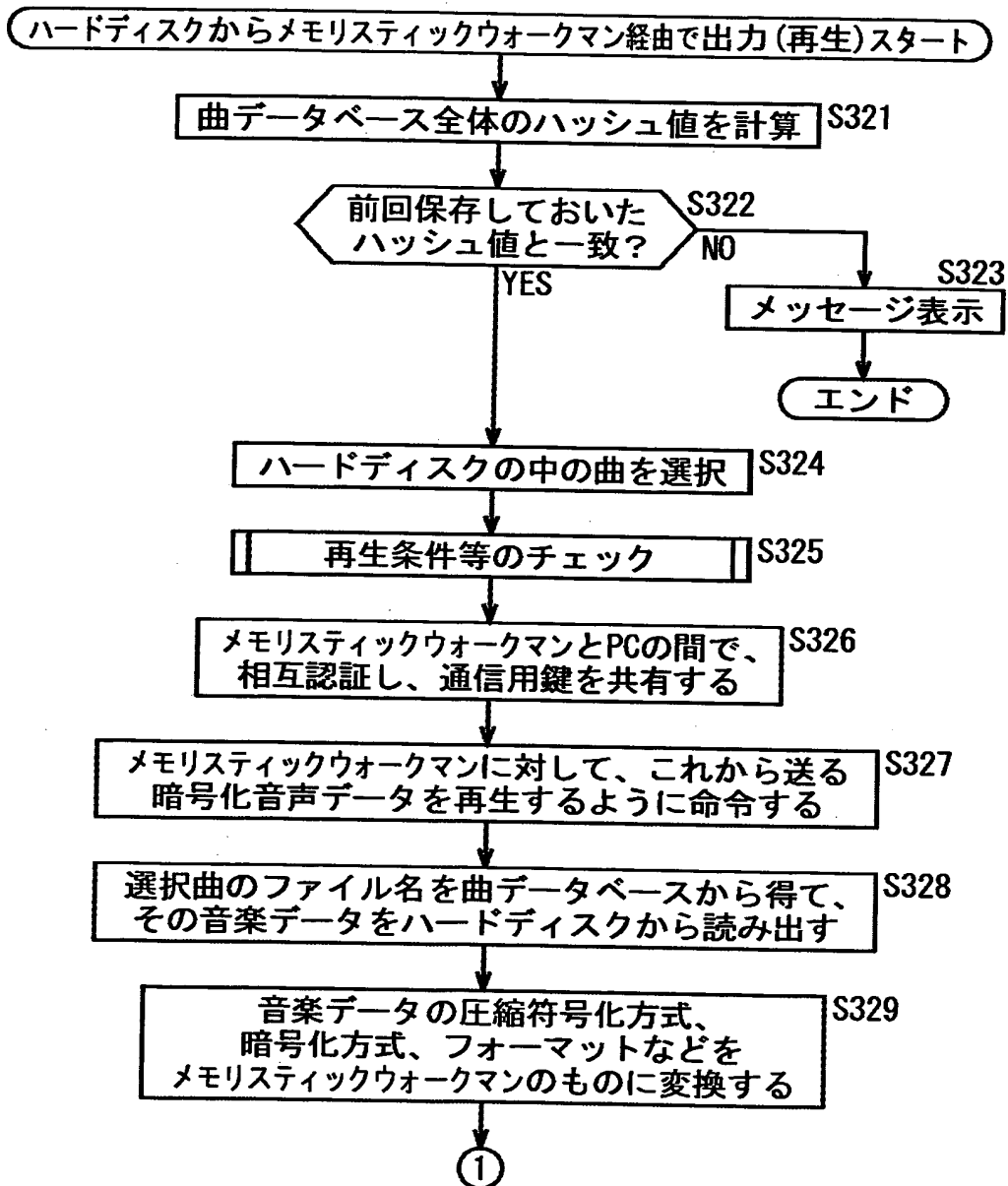
【図 24】



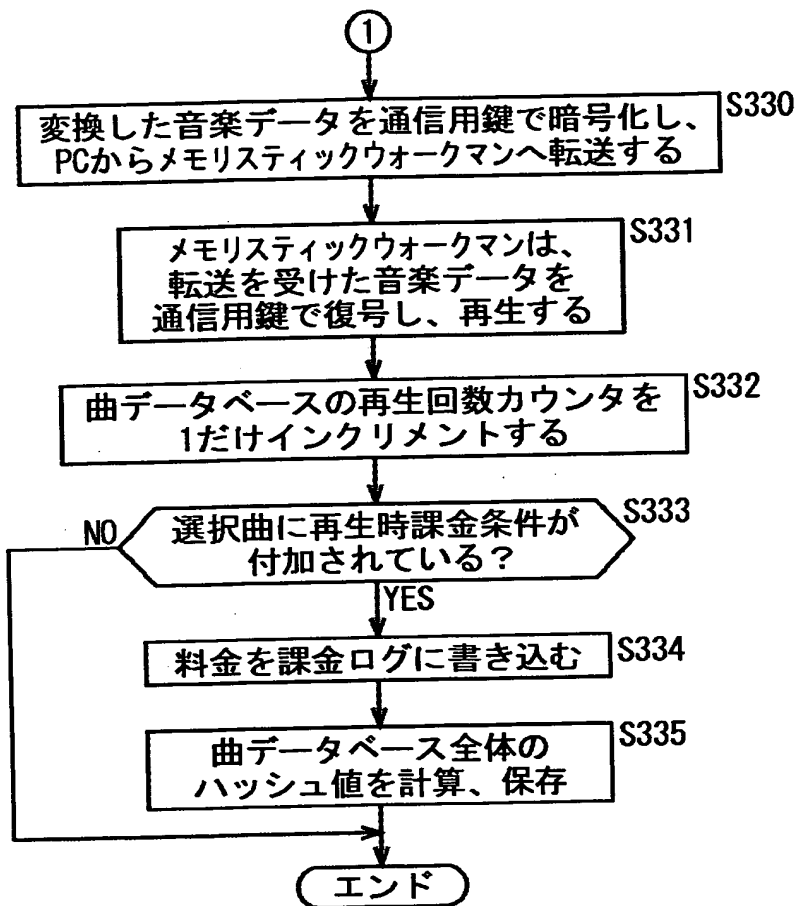
【図 25】



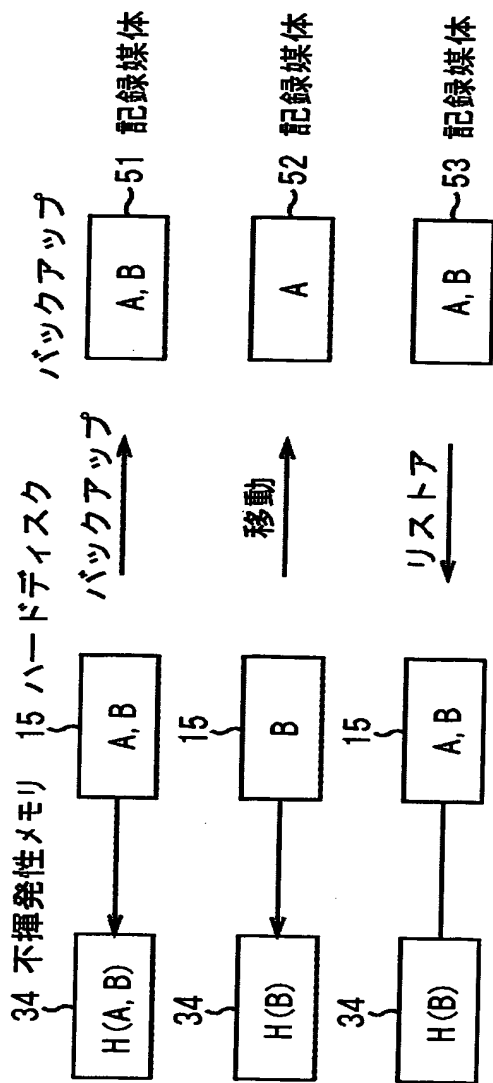
【図 26】



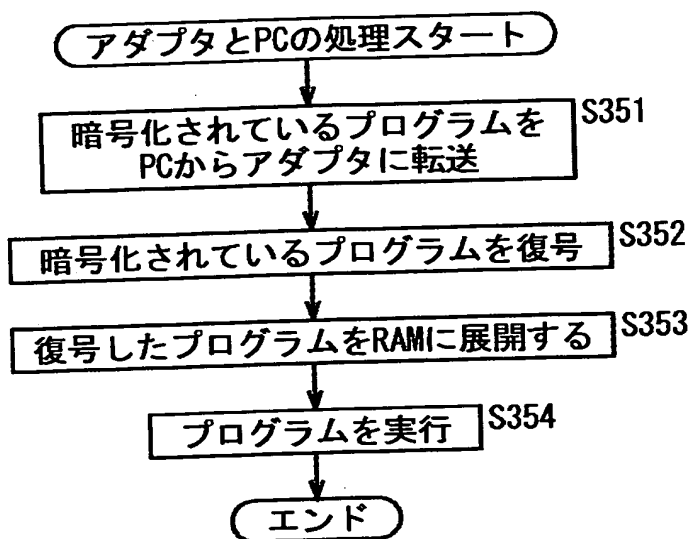
【図 27】



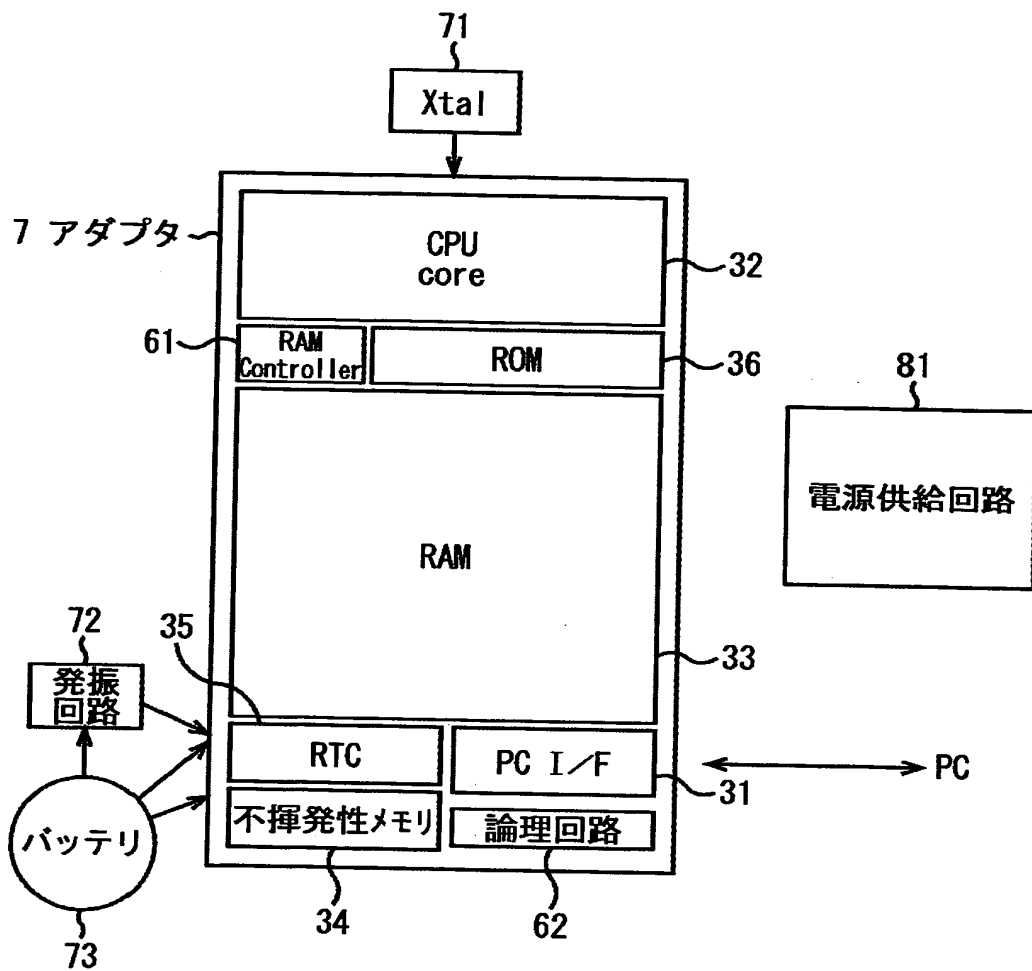
【図 28】



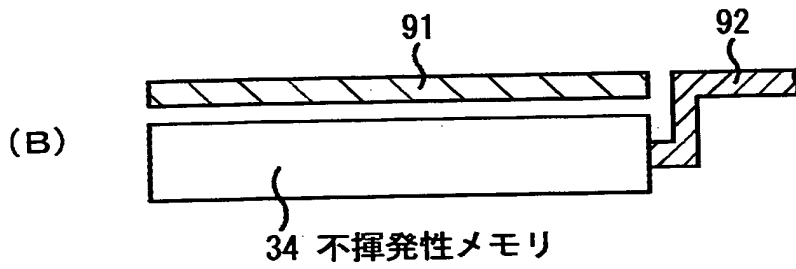
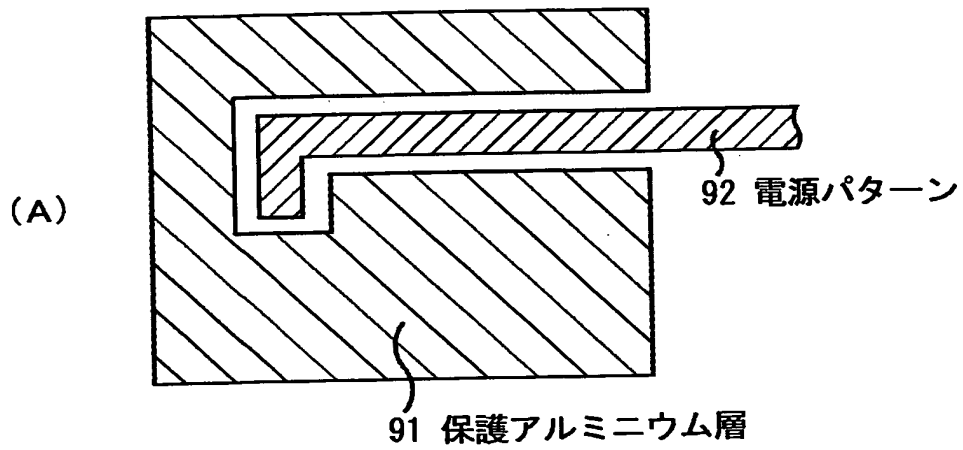
【図 2 9】



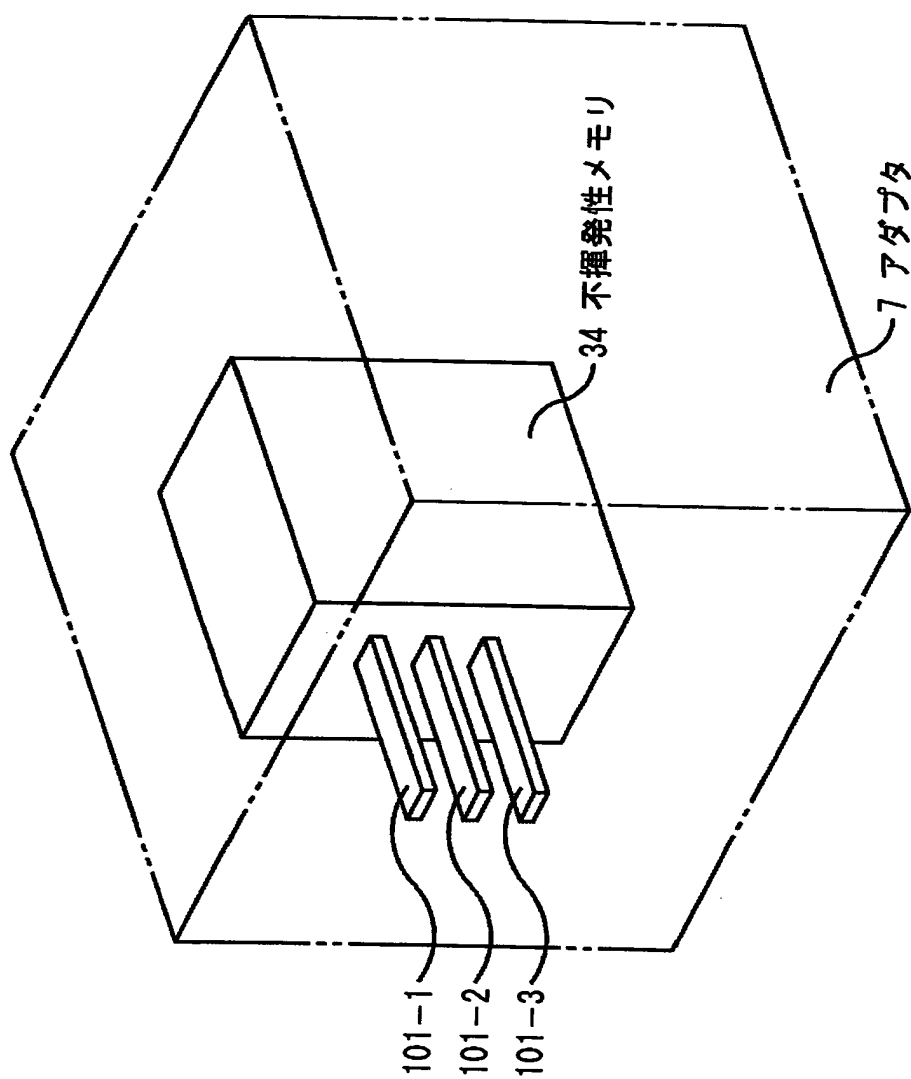
【図 3 0】



【図 31】

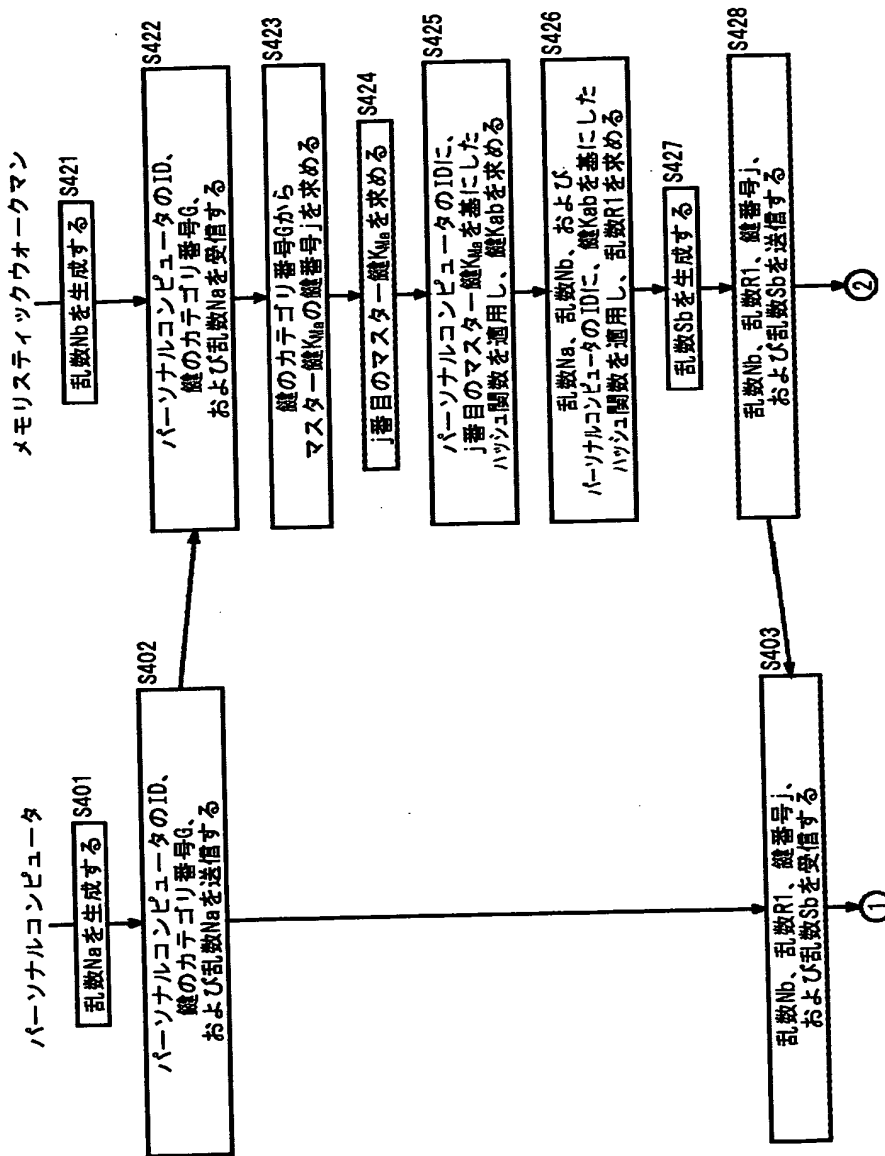


【図 3 2】



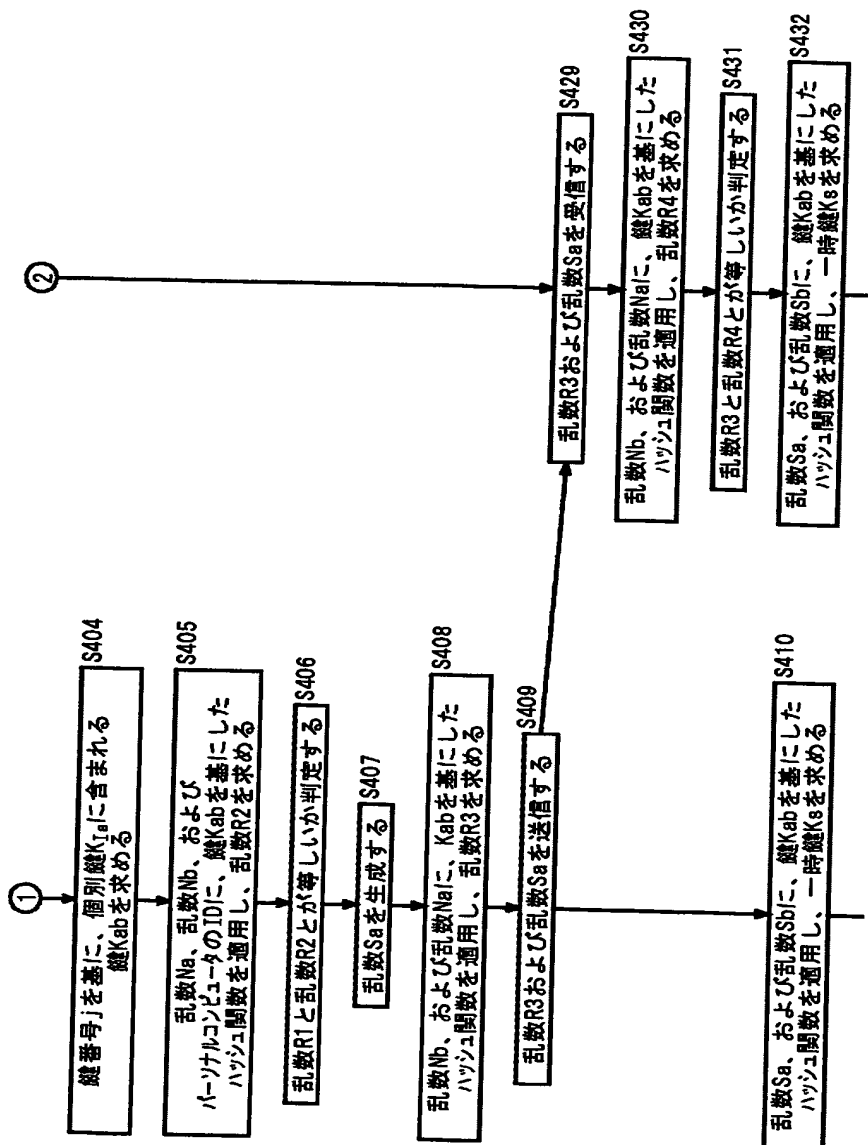
【図 3 3】

(33-1)



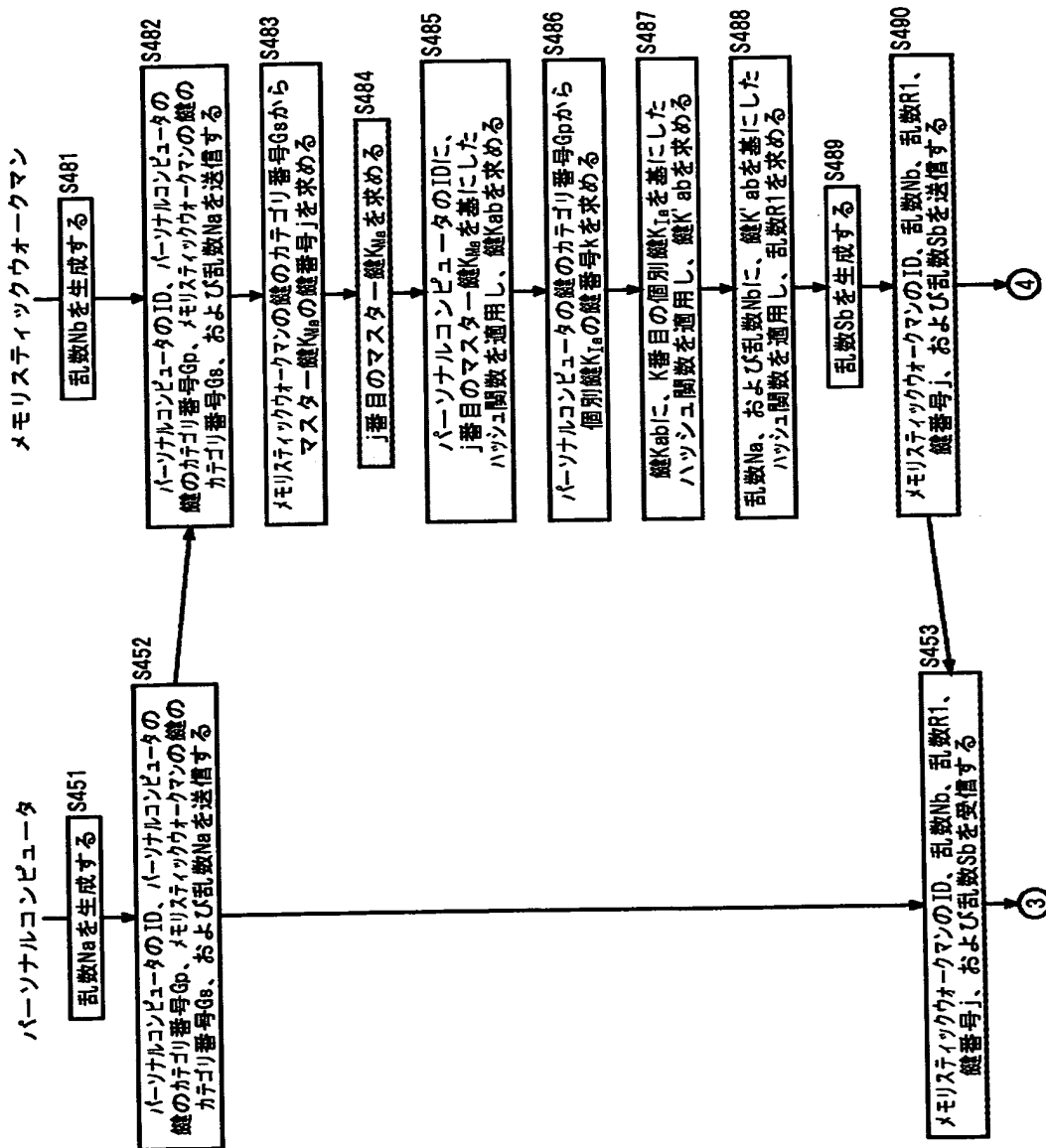
【図 3 4】

(33-2)



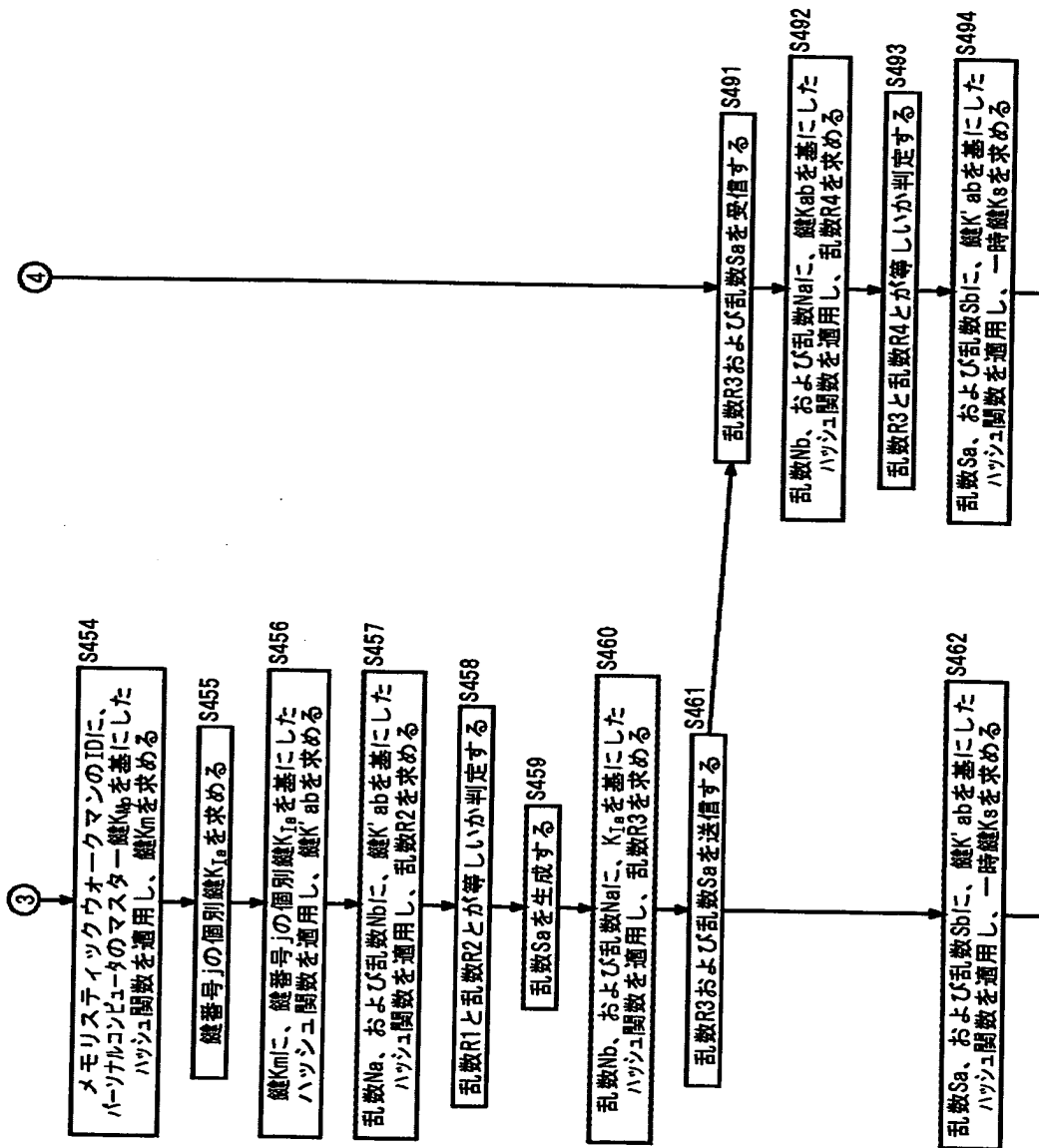
【図 3 5】

(35-1)

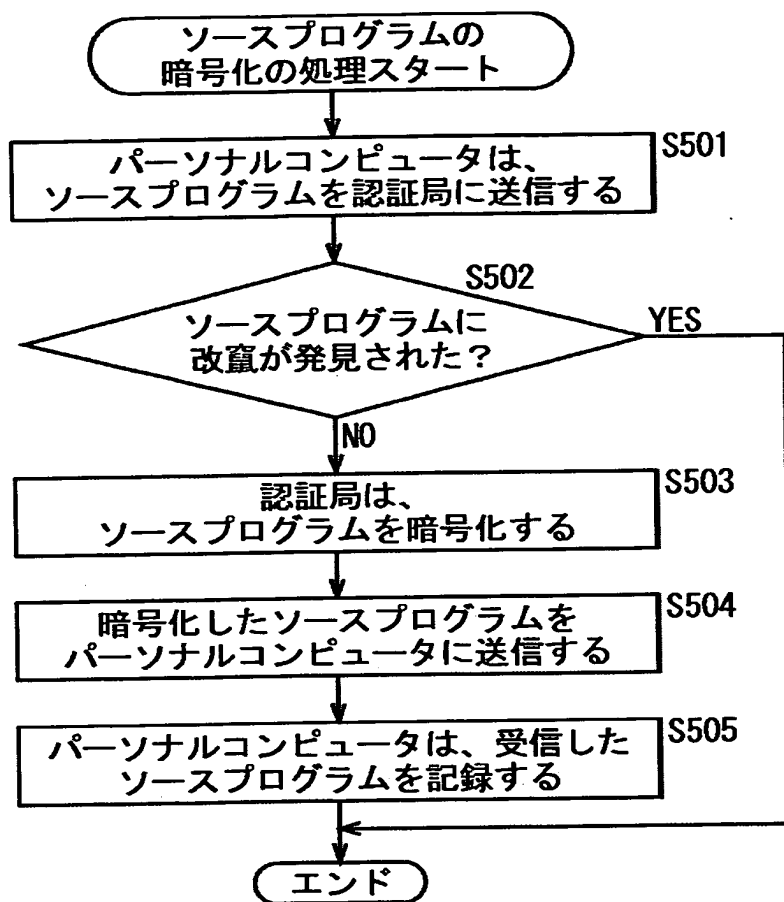


【図 3 6】

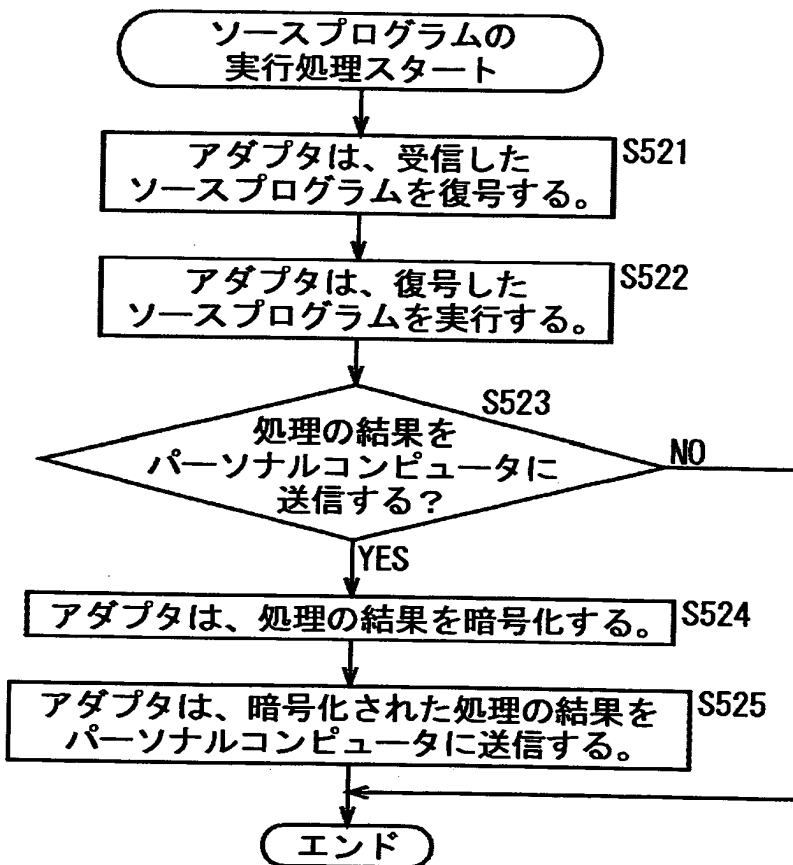
(35-2)



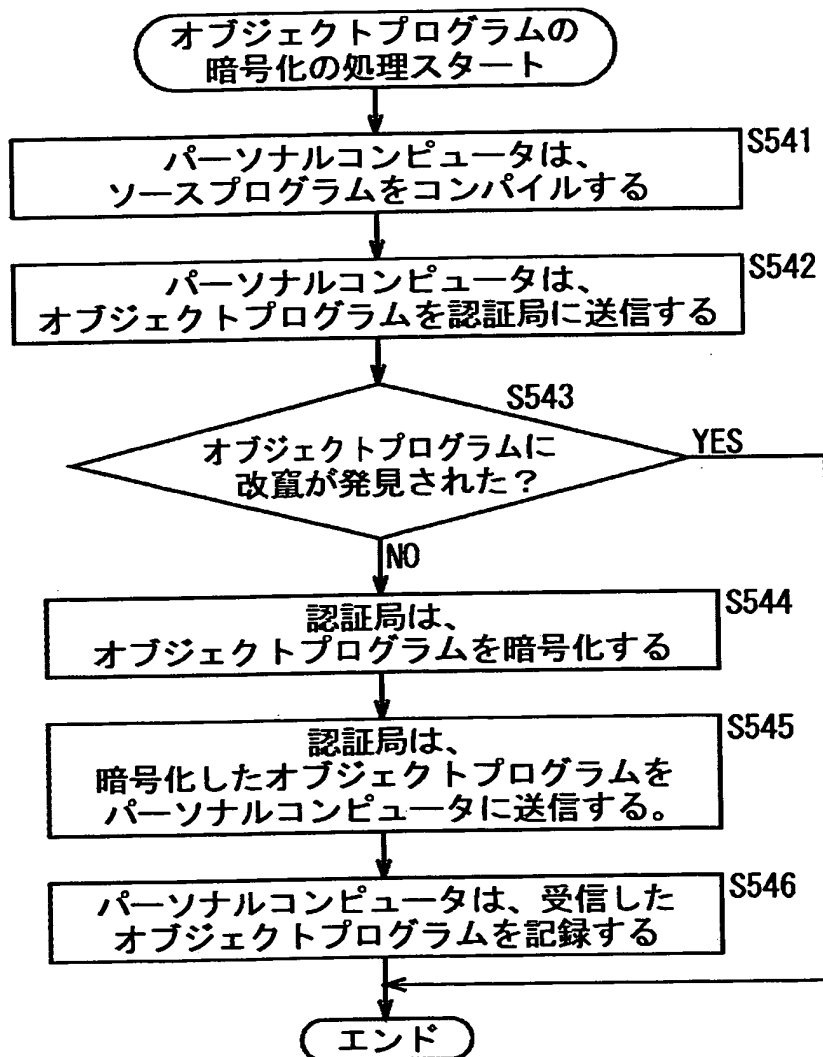
【図 37】



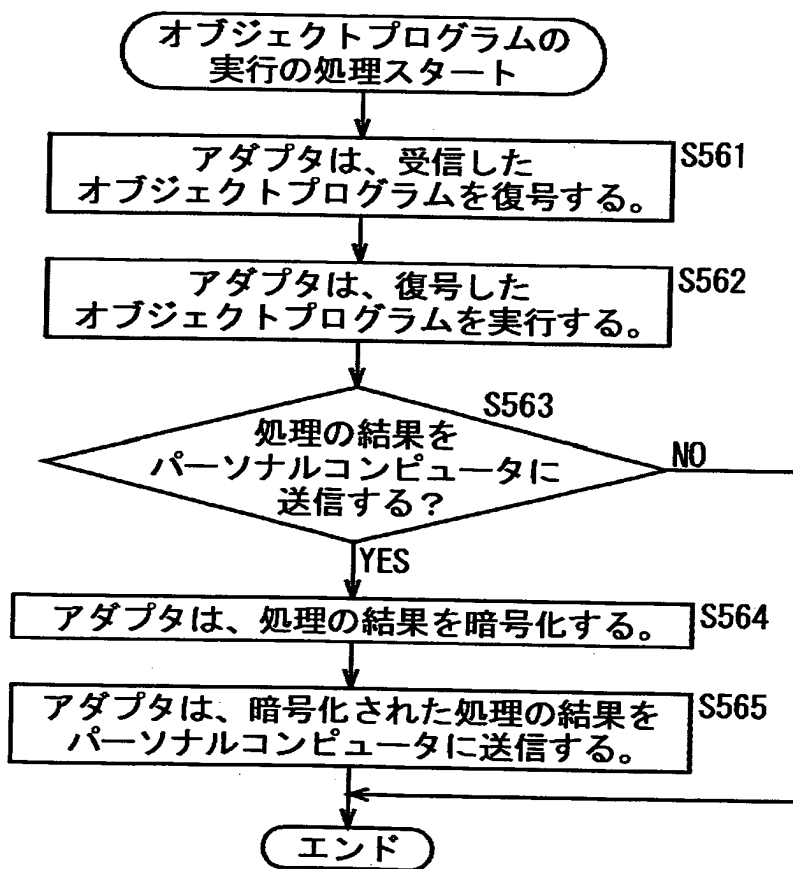
【図 38】



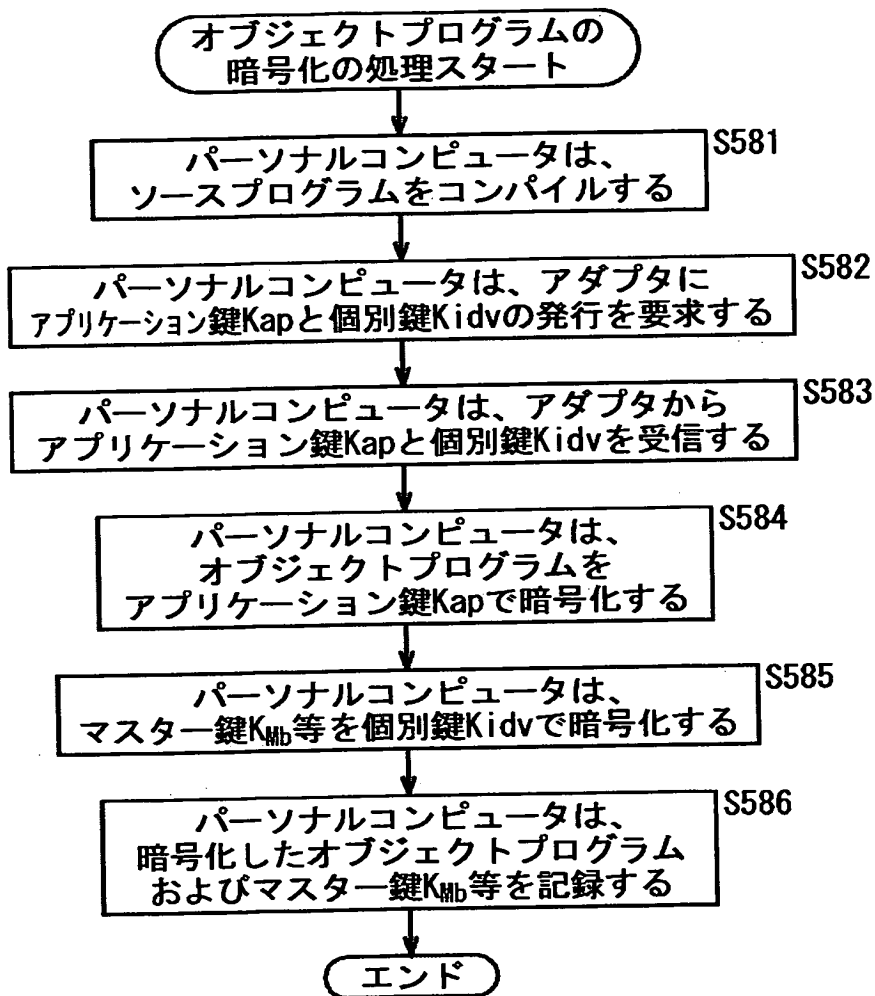
【図 39】



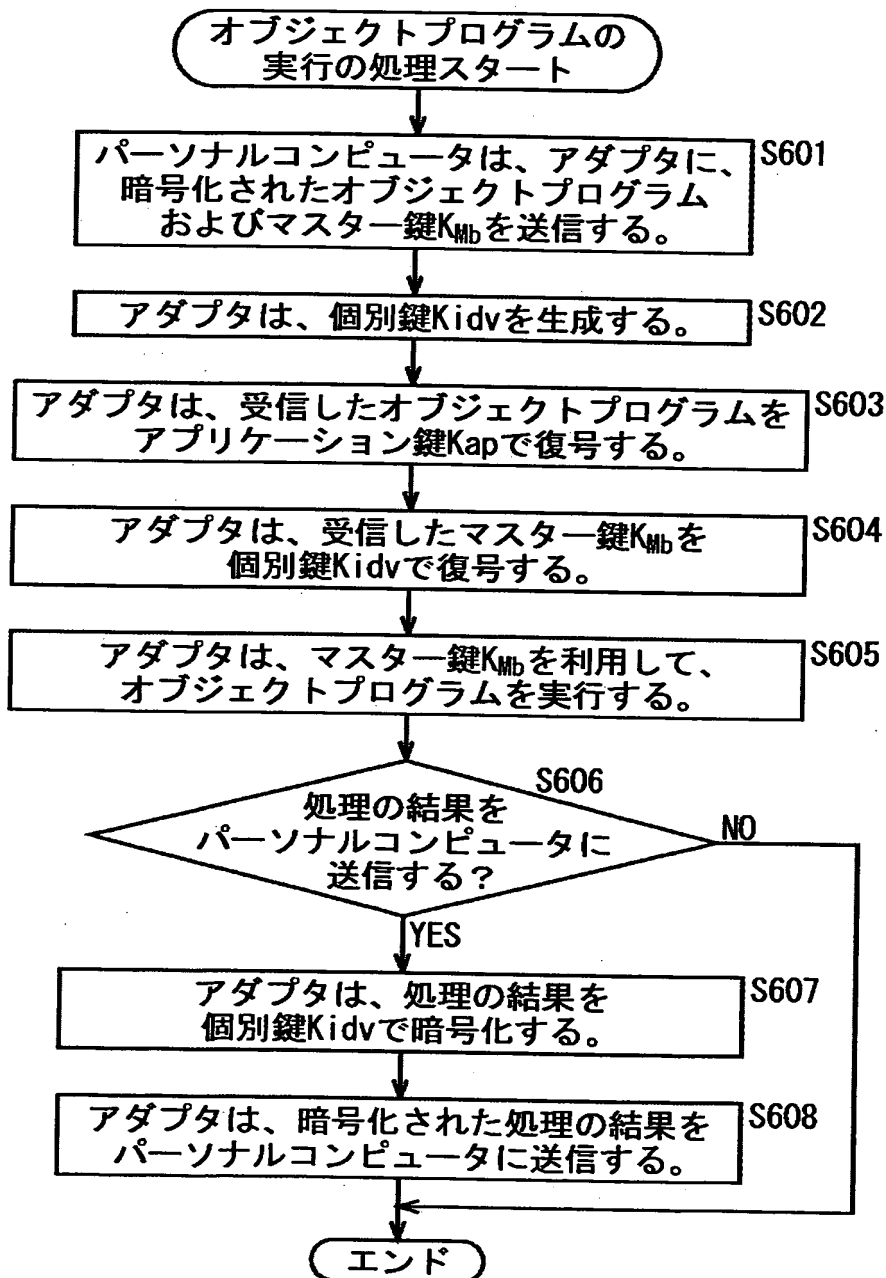
【図 40】



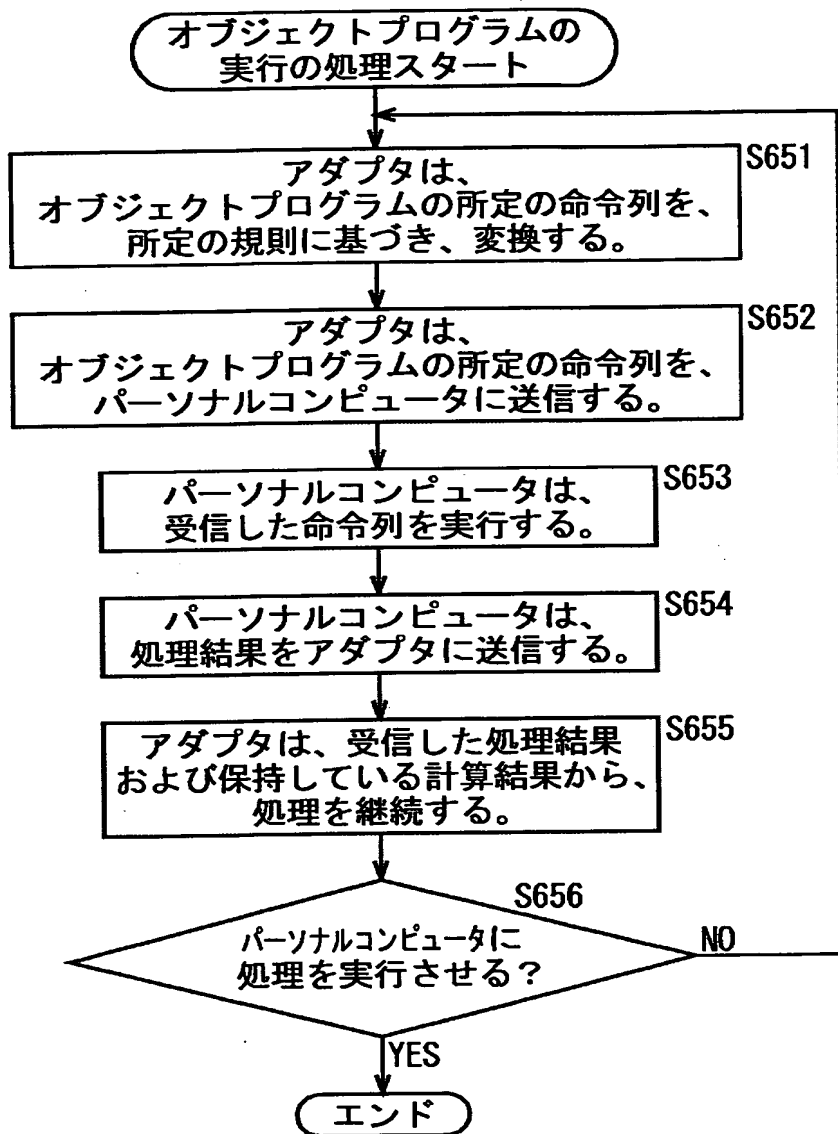
【図 4 1】



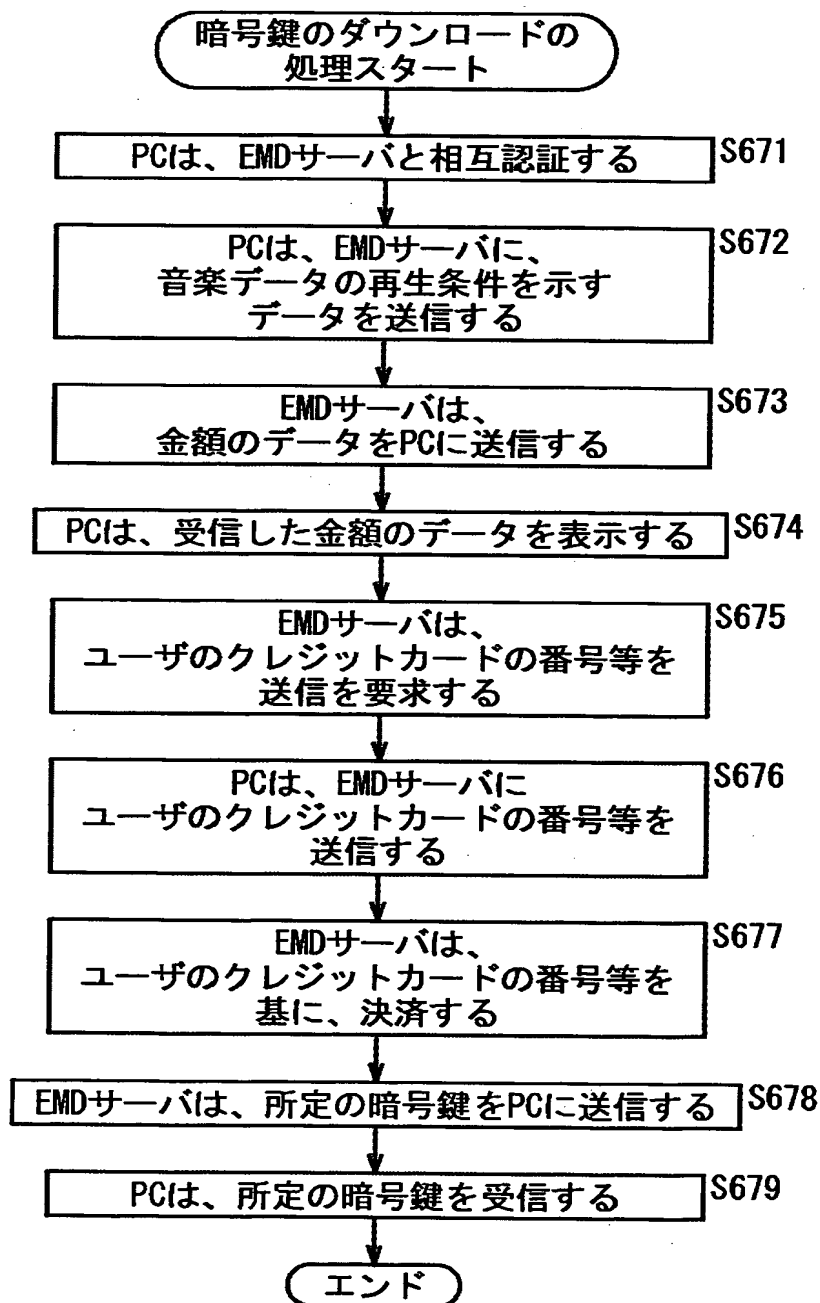
【図 4 2】



【図 43】



【図 4 4】



【書類名】 要約書

【要約】

【課題】 記憶されているデータが不正に読み出され、解析されるのを防止する

。 【解決手段】 インターネット接続インターフェース 11 は、アダプタ 7 に実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する。ハードディスク 15 は、認証局から受信した、暗号化されたプログラムを記録する。インターフェース 17 は、ハードディスク 15 に記録されているプログラムを、アダプタ 7 に送信する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都品川区北品川6丁目7番35号

氏 名

ソニー株式会社